Chapter 3: IT OPERATIONS

Introduction:

For banks in which information technology (IT) systems are used to manage information, IT Operations should support processing and storage of information, such that the required information is available in a timely, reliable, secure and resilient manner.

IT Operations are a set of specialized organizational capabilities that provide value to customers (internal or external) in form of IT services. Capabilities take the form of functions and processes for managing services over technology lifecycle. IT Operations should ensure effectiveness and efficiency in delivery and support of these services to ensure value for customers.

Scope:

Functions covered as a part of IT Operations are:

- IT Service Management
- Infrastructure Management
- Application Lifecycle Management
- IT Operations Risk Framework

The Board, Senior Management:

- Roles and Responsibilities:

Bank's Board of Directors has ultimate responsibility for oversight over effective functioning of IT operational functions. Senior management should ensure the implementation of a safe IT Operation environment. Policies and procedures defined as a part of IT Operations should support bank's goals and objectives, as well as statutory requirements.

- Functional areas, within the preview of these roles, are*:*

- Core IT Operations
- Business Line-specific IT Operations
- Any Affiliates-related IT Operations
- Business Partners' Operations (including that of IT support vendors if any)

The Board or Senior Management should take into consideration the risk associated with existing and planned IT operations and the risk tolerance and then establish and monitor policies for risk management.

Organisational Structure*:*

IT Operations include business services that are available to internal or external customers using IT as a service delivery component–such as mobile or internet banking. IT Operations include components that are used to support IT Operations: service desk application, ticketing and event management tools, etc. Banks may consider including Test and Quality Assurance Environment (besides, Production Environment) within the scope of IT Operations.

a) **Service Desk*:*** The service desk is the primary point of contact (Single Point of Contact or SPOC) for internal and external customers. Besides handling incidents and problems, it also provides interface to other IT operation processes, such as

Request For Change (RFC), Request Fulfilment, Configuration Management, Service Level Management and Availability Management, etc. It can have the following functions:

- Interacting with customers (e-mail, voice or chat): first-line customer liaison
- Recording and tracking incidents and problems or requests for change
- Keeping customers informed on request status and progress
- Making an initial assessment of requests, attempting to resolve them via knowledge management or escalating, based on agreed service levels
- Monitoring and escalation procedures relative to the appropriate SLA
- Managing the request life-cycle, including closure and verification
- Co-ordinating second-line and third-party support groups
- Providing management information for service improvement
- Identifying problems
- Closing incidents and confirmation with the customer
- Contributing to problem identification
- Performing user satisfaction surveys

A structure for the Service Desk that allows optimum resource utilization would include*:*

- Local Service Desk
- Central Service Desk
- Virtual Service Desk
- Follow the Sun i.e. in time zones such that service desk is available for assistance and recording of incidents round the clock
- Specialized Service Desk Groups

b) **<u>IT Operations Management</u>**

i. IT Operations management is a function which is primarily responsible for the day-to-day management and maintenance of an organisation's IT infrastructure, ensuring service delivery to the agreed level as defined by Service Level Agreement (SLA).

ii. IT Operations management can have following functions:

- **Operational Control:** Oversee the execution and monitoring of operational activities and events in IT infrastructure which is within the preview of IT operations. Operational control activities are normally carried out by Network Operations Centre (NOC) or Operations Bridge. Beside execution and monitoring of routine tasks operation control also involve the following activities :

- *Console Management*
- *Job Scheduling*
- *Backup and Restoration*
- *Print and Output Management*
- *General Maintenance Activities*

- **Facility Management:** It refers to management of physical IT environment of

data centre, computers rooms and recovery sites

iii. Operations Management Structure: For all practical reasons, application management and infrastructure management teams should be part of IT operations. As, these functions manage and execute operational activities, whereas others delegate these to dedicate IT operations function.

c) **Application Management:**

It involves handling and management of application as it goes through the entire life-cycle. The life-cycle encompasses both application development and application management activities. Sub-activities that can be defined for application management functions are:

- **Application Development:** It is concerned with activities needed to plan, design and build an application that ultimately is used by a part of the organisation to address a business requirement. This also includes application acquisition, purchase, hosting and provisioning
- **Application Maintenance/Management:** It focuses on activities that are involved with the deployment, operation, support and optimisation of the application

Application Management related functions may include the following:

- Managing operational applications, whether vendor developed, or off-the-shelf or in-house
- It acts as a custodian of technical knowledge and expertise related to managing and supporting applications. It ensures that the technical knowledge and expertise required to design, develop, test, manage and improve IT services are identified, developed and refined. Therefore, it participates in IT operation management
- It ensures that appropriate resources are effectively trained and deployed to deliver, build, transit, operate and improve the technology required to manage and support IT services
- It defines and executes training programmes
- It documents skill sets available within an organisation and skills that need to be developed to manage application management as function
- It defines standards to be adapted when defining new application architecture and involvement in design and build of new services
- It assesses the risk involved in an application architecture
- It records feedbacks on availability and capacity management activities
- It designs and performs tests for functionality, performance and manageability of IT services
- It defines and manages event management tools
- It participates in incident, problem, performance, change and release managament, and in resource fulfillment
- It provides information on the Configuration Management System

Application Management Structure: Though activities to manage applications are generic and consistent across applications; application management function, for all practical reasons, is not performed by a single department or group. It consists of technical areas as per technical skill sets and expertise. Some of these can be:

- Financial application
- Infrastructure applications

- Messaging and collaborative applications
- Web portal or web applications
- Contact centre applications
- Function-specific applications

d) **Infrastructure Management**

It is the function primarily responsible for providing technical expertise and overall management of the IT infrastructure. Its primary objective is to assist in plan, implement and maintenance of a stable technical infrastructure in order to support an organisation's business processes.

Infrastructure Management can have following functions:

i. Manage IT infrastructure components for an environment, which falls within the preview of IT operations

ii. It acts as a custodian of technical knowledge and expertise, related to the management of IT infrastructure. It ensures that technical knowledge and expertise required to design, develop, test, manage and improve IT services are identified, developed and refined

iii. It ensures appropriate resources are effectively trained and deployed to deliver, build, transit, operate and improve the technology required to deliver and support IT infrastructure

iv. It helps define and execute training programmes

v. It helps document skill sets available within an organisation and skills needed to be developed to manage infrastructure management as function

vi. Definition of standards to be adapted when defining new IT architecture and involvement in the design and build of new services

vii. Risk assessment for IT infrastructure architecture

viii. Feedbacks to availability and capacity management activities

ix. Designing and performing tests for functionality, performance and manageability of IT services

x. Definition and management of event management tools

xi. Participation in incident, problem, performance, change and release management and resource fulfillment

xii. Infrastructure management function should provide information or manage for configuration Management System

Infrastructure Management Structure**:** For all practical reasons, infrastructure management function is not performed by a single department or group, it consist of technical areas as per the technical skill sets and expertise, some of these are:

- Mainframe management team
- Server management team
- Storage management team
- Network support team
- Desktop support team
- Database management team
- Middleware management team

- Directory services team
- Internet team
- Messaging team
- IP-based telephony team

Components of IT operations framework:

a) Risk Management

Banks should analyse their IT Operation environment, including technology, human resources and implemented processes, to identify threats and vulnerabilities. They should conduct a periodic risk assessment which should identify:

- *Internal and external risks*
- *Risks associated with individual platforms, systems, or processes, as well as automated processing units*

While identifying the risks, a risk assessment process should quantify the probability of a threat and vulnerability, and the financial consequences of such an event. Banks should also consider the inter-dependencies between risk elements, as threats and vulnerabilities have the potential to quickly compromise inter-connected and inter-dependent systems and processes.

Banks should implement a cost-effective and risk-focused environment. The risk control environment should provide guidance, accountability and enforceability, while mitigating risks.

Risk Categorisation**:** As a part of risk identification and assessment, banks should identify events or activities that could disrupt operations, or negatively affect the reputation or earnings, and assess compliance to regulatory requirements. Risks identified can be broadly categorised into following categories:

- *Strategic Failures:* That might include improper implementation, failure of supplier, inappropriate definition of requirements, incompatibility with existing application infrastructure etc. It will also include regulatory compliance
- *Design Failures:* It might include inadequate project management, cost and time overruns, programming errors and data migration failures among others
- *Transition Failures:* It might include inadequate capacity planning, inappropriately defined availability requirements, SLA / OLA / Underpinning contracts not appropriately defined and information security breaches, among others

Risk Mitigation**:** Once the organisation has identified, analyzed and categorized the risks, organisation should define following attributes for each risk component:

- Probability of Occurrence;
- Financial Impact;
- Reputational Impact;
- Regulatory Compliance Impact;
- Legal Impact.

Beside above specified attributes, an organisation should also consider these:

- Lost revenues
- Loss of market share

- Non-compliance of regulatory requirements
- Litigation probability
- Data recovery expenses
- Reconstruction expenses

These, along with the business process involved, should be used to prioritise risk mitigation actions and control framework.

b) IT Operations Processes

i) IT Strategy

Processes within IT Strategy provide guidance to identify, select and prioritise services that are aligned to business requirements. IT strategy, as a framework, provides feedback to IT Operations on the services to be supported and their underlying business processes and prioritisation of these services, etc.

A well-defined IT Strategy framework will assist IT Operations in supporting IT services as required by the business and defined in OLA / SLAs.

IT Strategy processes provide guidelines that can be used by the banks to design, develop, and implement IT Operation not only as an organisational capability but as a strategic asset.

a) Financial Management: It provides mechanism and techniques to IT operations to quantify in financial terms, value of IT services it supports, value of assets underlying the provisioning of these services, and qualification of operational forecasting.

Advantages of implementing Financial Management process are:

- Assists in decision-making
- Speed of changes
- Service Portfolio Management
- Financial compliance and control
- Operational control
- Value capture and creation

b) Service Valuation

It is the mechanism that can be used by banks to quantify services, which are available to customers (internal or external) and supported by IT operations in financial terms. It assists IT Operation functions to showcase the involvement of function in supporting the bank's core business.

Financial Management uses Service Valuation to quantify financial terms, value of IT services supported by IT Operations. It provides a blueprint from which businesses can comprehend what is actually delivered to them from IT. Combined with Service Level Management, Service Valuation is the means to a mutual agreement with businesses, regarding what a service is, what its components are, and its cost and worth.

Service Valuation quantifies, in financial terms, funding sought by a business and IT for services delivered, based on the agreed value of those services. The activity involves identifying cost baseline for services and then quantifying the perceived valued, added by the provider’s service assets in order to conclude a final service value.

Service Valuation will have two components, these being:

i) Provisioning Value: The actual underlying cost of IT, related to provisioning a service, including all fulfillment elements–tangible and intangible. Input comes from

financial systems and consists of payment of actual resources consumed by the IT in the provisioning of services. This cost element includes items such as:

- *Hardware and software licence cost*
- *Annual maintenance fees for hardware and software*
- *Personnel resources used in the support or maintenance of the services*
- *Utilities, data centre or other facilities charge*
- *Taxes, capital or interest charges*
- *Compliance costs*

ii) Service Value Potential: Is the value-added component based on a customer's perception of value from the service or expected marginal utility and warranty from using the services in comparison with what is possible using the customer's own assets.

c) Portfolio Management

It provides guidelines that can be used by banks for governing investments in service management across an enterprise and managing them for value. Portfolio management contains information for all existing services, as well as every proposed service–those that are in conceptual phase.

Every service, which is a part of service portfolio, should include a business case, which is a model of what a service is expected to achieve. It is the justification for pursuing a course of action to meet stated organisational goals. Business case links back to service strategy and funding. It is the assessment of a service management in terms of potential benefits and the resources and capabilities required to provision and maintain the service. Portfolio Management framework defined by the banks should highlight controls, which are defined to develop an IT Service from conceptual phase to go-live phase and then to transition to production environment. During the development of IT services financial impact of the new service on IT Operation should also be ascertained which will assist IT Operations in Service Validation.

d) Demand Management

Demand Management process provides guidelines which can be used by banks to understand the business processes IT operations supports to identify, analyse, and codify Patterns of business activities (PBA) to provide sufficient basic for capacity requirement. Analysing and tracking the activity patterns of the business process makes it possible to predict demand for services. It is also possible to predict demand for underlying service assets that support these services.

Demand Management guidelines should also take into consideration IT Operations involvement in development of service from conceptual phase to go to the live phase, so that there is a transparency of demand of new service in IT Operations.

ii) Design

The design phase of the IT operations provides the guidelines and processes, which can be used by the banks to manage the change in the business landscape. Components which should be considered when designing a new IT service or making a change to the existing IT service are:

- Business Processes
- IT Services
- Service-level Agreements
- IT Infrastructure

- IT Environment
- Information Data
- Applications
- Support Services
- Support Teams
- Suppliers

i) **Service design:** This should not consider components in isolation, but must also consider the relationship between each of the components and their dependencies on any other component or service.

ii) **Design phase:** Provides a set of processes and guidelines that can be used by banks to design IT services, supported by IT operations, that satisfies business objectives, compliance requirements and risk and security requirements. The processes also provide guidelines to identify and manage risks and to design secure and resilient IT services.

e) Service Catalogue Management

Over the years, banks' IT infrastructure has grown and developed. In order to establish an accurate IT landscape, it is recommended that an *IT Service Catalogue* is defined, produced and maintained. It can be considered as a repository that provides information on all IT services supported by IT Operations framework.

The Service Catalogue Management process provides guidelines, used by banks to define and manage service catalogue, which provides a consistent and accurate information on all IT services available to customers (internal or external). It also ensures that the service catalogue is available to users, who are approved to access it. It should contain details of all services that are in production, as well as the services that are being prepared for transition. Banks should consider attributes to be included into the service catalogue:

1. Definition of Service
2. Categorization of Service (business application and IT support)
3. Service Criticality
4. Disaster Recovery Class
5. Service-level Agreement Parameters
6. Service Environment (Production, Testing, Quality Assurance, Staging, etc.)
7. IT Support Status (Operational and Transaction, etc.)
8. Configuration Management Group
9. Incident Management Group
10. Problem Management Group
11. Change and Release Management Group
12. Service Owner
13. Service-level Manager
14. Principal Business Activities Details
15. Interdependency on Configuration Items
16. Interdependency on Service Portfolio

Service catalogue provides details of services available to customers such as intended use, business processes they enable and the level and quality of service the customer can expect

from each service. Banks can also consider incorporating "charge back mechanism", as defined in financial management into the service catalogue.

A Service catalogue has two aspects:

i) **Business Service Catalogue:** It contains details of all IT services delivered to a customer, together with relationships with business units and business processes that rely on IT services. This is the customer view of the catalogue. Business Service Catalogue facilitates development of robust Service Level Management process.

ii) **Technical Service Catalogue:** It contains details of all IT services delivered to a customer, together with his or her relationship with supporting and shared services, relationship to configuration items (CIs). CIs can be a service asset or component, or any other item that is under control of configuration management. Depending on established strategy configuration, an item may vary widely in complexity, sise and type. It can range from entire services or systems to a single software module or a minor software component. (Configuration Items are explained in details in "Service Assets and Configuration Management" section of the guidelines.) It facilitates the development of the relationship between services, underlying CIs, SLAs and OLAs, and the support groups, which support services throughout its life-cycle.

f) Service Level Management

This process defines the framework that can be used by banks to plann, co-ordinate and draft, agree, monitor and report service attributes used to measure the service quality. Its framework also includes guidelines for ongoing review of service achievements to ensure that the required and cost-justifiable service quality is maintained and improved. Beside current services and SLAs, this management provides guidelines to ensure that new requirements are captured. That new or changed services and SLAs are developed to match the business needs and expectations.

i) Service Level Management process should be able to meet the following objectives:

- Define, document, agree, monitor, measure, report and review the level of IT services
- Ensure specific and quantifiable targets are defined for IT services
- Ensure that IT Operations and consumers have clear, unambiguous expectations of the level of services to be delivered
- Ensure that pro-active measures, to improve the level of service delivered, are implemented if cost-justified

ii) While defining SLM framework for banks, the following aspects should also be considered

- Operational-level agreement to ensure that Operational Level Agreements (OLAs) with other support groups are defined and developed; these OLAs should be in line with SLAs which it supports
- Underpinning supplier contract to ensure all underpinning supplier contracts with the vendors or suppliers are defined and developed: these contracts should be in line with SLAs, which it supports

iii) While defining Service Level Agreement as a part of Service Level Management framework, the following options can be considered:

- **Service based SLA:** Its structure covers attributes for single service across an organisation. For instance, SLA for internet banking service
- **Customer based SLA:** The structure covers attributes for all services for a defined set of customers. For instance, SLA for SMEs customers
- **Multi-Level SLA:** Multi-level SLA structure can be defined as per the organizational

hierarchy. For instance, SLA for corporate offices, branches and head offices

Attributes that are included in SLAs should be ones which can effectively be monitored and measured. Attributes which are included in the SLAs can be categorised into operational, response, availability and security attributes. Service Level Management framework should also define guidelines for reviews of Service Level Agreements, Operational Level Agreements, and underpinning contracts to ensure that they are aligned to business needs and strategy. These should ensure that services covered, and targets for each, are relevant. And that nothing significant is changed that invalidates the agreement in any way. Service Level Management framework defined should also have guidelines defined for logging and management, including escalation of complaints and compliments.

g) Capacity Management

The process provides the framework and guidelines that can be adapted by banks to ensure that cost-justifiable IT capacity exists and matches to current- and future-agreed business requirements as identified in Service Level Agreement.

The Capacity Management process provides guidelines to:

- Produce and maintain capacity plan that reflects the current and future business requirements
- Manage service performance so that it meets or exceeds the agreed performance targets
- Diagnosis and resolution of performance and capacity-related incidents and problems
- Assess impact of all changes on capacity plan and performance of IT services supported by IT Operations
- Ensure that pro-active measures are undertaken to improve the performance of services, whenever it is cost-justifiable.

One of the key activities defined as a part of capacity management process is to produce and maintain, at an ongoing basis, the capacity plan, which depicts current level of resource utilization and service performance. Capacity plans can also include forecasting future requirements to support business activities. *The process can be subdivided into three:*

i. **Business Capacity Management:** Defines guidelines for translating business-need plans into requirements for IT services and supporting infrastructure, ensuring that the future business requirements for IT services are quantified, designed, planned and implemented. Inputs for future IT requirements come from the Service Portfolio and Demand Management.

ii. **Service Capacity Management:** This defines guidelines for management, control and prediction of end-to-end performance and capacity of live and operational IT service usage and workloads. It provides guidelines to ensure that the performance of IT services is monitored and measured.

iii. **Component Capacity Management:** It defines guidelines to identify and understand the performance, capacity and utilization of each individual component within a technology used to support IT services, including infrastructure, environment, data and applications.

A major difference between sub-processes is in the data that is being monitored and collected. For example, the level of utilization of individual components in the infrastructure: processors, disks and network links will be under Component Capacity Management. While transaction throughput rates and response times will be under Service Capacity Management. Business Capacity Management will be concerned with data, specific to business volumes. Banks adapting capacity management process should ensure that its

framework encompass all areas of technology (hardware, software, human resource, facilities, etc.)

h) Availability Management

Availability and reliability of IT services can directly influence customer satisfaction and reputation of banks. Therefore Availability Management is essential in ensuring that the IT delivers the "right level" of service required by the business to satisfy its objectives. The process provides framework and guidelines that can be adapted by banks to ensure that the level of service availability (for all services) is matched, or exceeds the current and future requirements, as defined in the Service Level Agreement.

Availability Management process provides guidelines so that banks can:

- Produce and maintain an appropriate up-to-date Availability Plan that reflects the current and future needs of the business
- Ensure that service availability achievements meet or exceed agreed targets, by managing services and resources-related availability targets
- Assist with diagnosis and resolution of availability-related incidents and problems
- Ensure that pro-active measures to improve the availability of services are implemented wherever it is cost justifiable to do so

When implementing Availability Management processes, banks should consider including the following:

i. All operational services and technology, supported by IT Operations function and for which there is a formal SLA

ii. New services where Service Level Requirement and Agreement have been established

iii. Aspects of IT's services and components that may impact availability, which may include training, skills, process effectiveness, procedures and tools

Availability Management process has two key elements:

i. **Reactive activities:** The reactive aspect of availability management involves monitoring, measuring, analysis and management of events, incidents, problems and changes, involving unavailability

ii. **Proactive activities:** This aspect involves planning, design and improvement of availability

Attributes that can be used by the banks for reporting availability of IT services, can be:

- **Availability:** The ability of a service, component or CI, to perform the agreed function when required.

- **Availability (%) =** $\dfrac{\text{Agreed Service Time - Downtime}}{\text{Agreed Service Time}} \times 100$

  Downtime should only be included in the above calculation, when it occurs within the "Agreed Service Time".

- **Mean Time Between Service Incidents (MTBSI):** MTBSI refers to how long a service; component or CI can perform its agreed function without interruption.

- MTBSI = $\dfrac{\text{Available time in hours}}{\text{Number of Breaks}}$

- **Mean Time Between Failures (MTBF):** MTBF refers to how long a service; component or CI can perform its agreed function without reporting a failure.

$$MTBF = \frac{\text{Available time in hours – Total downtime in Hours}}{\text{Number of breaks}}$$

Mean Time Between Failures (MTBF): is the mean time between the recovery from one incident and occurrence of the next incident, it is also known as uptime. This metric relates to the reliability of the IT Service supported by IT Operations.

- **Mean Time to Repair (MTTR):** MTTR refers to how quickly and effectively a service, component or CI can be restored to normal working after failure.

$$MTTR = \frac{\text{Total downtime in Hours}}{\text{Number of breaks}}$$

Mean Time to Repair (MTTR): This is the average time between occurrence of a fault and service recovery. It is also known as downtime. This metric relates to the recoverability and serviceability of the IT Services supported by IT Operations.

Vital Business Functions

When defining availability targets for a business service, banks should consider identifying Vital Business Function (VBF). VBF represents critical business elements of a process supported by IT services. For example, an ATM will have following business functions:

i. Cash dispensing
ii. Reconciliation with the relevant account
iii. Statement printing.

Out of these three, cash dispensing and reconciliation should be considered as vital business functions, influencing the availability design and associated costs.

i) Supplier Management

Complex business demands require extensive skills and capabilities from IT to support business processes, therefore collaboration with service providers and value networks are an integral part of end-to-end business solution. Supplier Management process provides framework and guidelines that can be used by banks to manage relationships with vendors, suppliers and contractors. This framework ensures that suppliers and services they provide are managed to support IT service targets and business expectations. The purpose of this management process is to obtain value for money from suppliers, and to ensure that suppliers perform to the targets contained within contracts and agreements, while conforming to all terms and conditions.

Supplier Management process provides guidelines which can be used by the banks to:

- Implement and enforce supplier policies
- Maintenance of supplier and contact database
- Suppler and contact categorization and risk assessment

- Supplier and contract evaluation and selection
- Development, negotiation and agreement of contracts
- Contract review, renewal and termination
- Management of suppliers and supplier performance
- Agreement and implementation of service and supplier improvement plans
- Maintenance of standard contracts, terms and conditions
- Management of contractual dispute resolution
- Management of sub-contracted suppliers

iii) Transition

The transition phase provides frameworks and processes that may be utilised by banks to:

- Evaluate service capabilities and risk profile of new or changes service before it is released into production environment
- Evaluate and maintain integrity of all identified service assets and configuration items required to support the service

Service Asset and Configuration Management

Service Asset and Configuration Management process provides framework and guidelines that can be used by the banks to manage service assets and configuration items that supports business services.

The framework provides guidelines to:

- Identify, control, record, audit and verify service assets and configuration items, including service baseline version controls their attributes and relationships.
- Manage and protect integrity of service assets and configuration items through the service lifecycle by ensuring only authorised assets are used and only authorised changes are made.
- Ensure integrity of configuration items required to support business services and IT infrastructure by establishing and maintaining an accurate and complete Configuration Management System.
- Provide accurate information of configuration items to assist in change and release management process.

Service asset management manages assets across its lifecycle from acquisition through disposal. Implementation of Service Asset and Configuration Management framework has cost and resources implications and therefore strategic discussions needs to be made about the priorities to be addressed. For instance banks can decide on initially focusing on the basic IT assets (hardware and software) and the services and assets that are business critical or covered by legal regulatory compliance.

Components that can be considered as part of Service Asset and Configuration Management are:

i. **Configuration Items:** These can be a service asset or component, or any item that is under the control of configuration management. Depending on established strategy configuration, the item may vary widely in complexity, size and type. It can range from an entire service or system to a single software module or a minor software

component.

If desired, banks can define a hierarchical structure for configuration items. For instance banks can define Core Banking as a configuration item which can have different application as a subset Configuration Item of the Core Banking configuration item. Each configuration item can have modules as sub set which can have two configuration item, these being hosting and application support. Hosting can then be further sub-divided into configuration item that can be servers, operating systems, databases, network components.

ii. **Configuration Management System:** To manage large and complex IT environment banks may consider implementation of supporting system known as Configuration Management System. Beside holding information about configuration items, their components and relationship between configuration items Configuration Management System can also be used to correlate services and configuration items; this kind of snapshot will assist in proactively identifying incidents, events etc.

iii. **Secure libraries:** Secure library is a collection of software, electronic or document CIs. Access to items in a secure library is restricted. The secure library is used for controlling and releasing components throughout the service lifecycle.

iv. **Definitive Media Library:** Definitive media library (DML) is a secure library that may be used to store definitive authorised versions of all media CIs. It stores master copies of versions that have passed quality assurance checks.

v. **Configuration Baseline:** This baseline is the configuration of a service, product or infrastructure that has been formally reviewed and agreed on, that thereafter serves as the basis for further activities and that can be changed only through formal change procedure. Configuration baseline captures and represents a set of configuration items that are related to each other.

vi. **Snapshot:** It defines the current state of configuration items or an environment.

vii. **Change Management:** This process provides guidelines which can be used by the banks for handling changes to ensure that the changes are recorded, assessed, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner and environment. The primary objective of the change management procedures is to ensure assessment of:

- Risks
- Change authorization
- Business Continuity
- Change impact

iv) Operations

This phase, as a part of Service Management lifecycle, is responsible for executing and performing processes that optimise the cost of the quality of services. As a part of the organisation, it's responsible for enabling businesses to meets objectives. As a part of technology, it's responsible for effective functioning of components that support business services.

Event Management

Event Management process provides the guidelines which can be used by the banks to define the framework for monitoring all the relevant events that occurs through the IT infrastructure. It provides the entry point for the execution of many Service Operations processes and activities.

Event can be defined as any detectable or discernible occurrence that has significance for the management of the IT infrastructure, or delivery of IT services. *Event Management framework when defined will have two mechanisms for monitoring, these are:*

- **Active Monitoring:** Active monitoring is related to polling of business significant Configuration Items to determine their status and availability. Any diversion from normal status should be reported to appropriate team for action.
- **Passive Monitoring:** Passive monitoring detects and correlate operational alerts or communications generated by Configuration Items.

Event Management can be applied to any aspect of Service Management that needs to be controlled. These components can be:

- Configuration Items
- Environment conditions
- Software licence monitoring
- Security breaches

Event Management portfolio can have different kind of event, some of these are:

- **Informational:** Events signifying regular operations for instance notification that a scheduled job has completed
- **Warning:** Events signifying diversion from normal course of action, for instance a user attempting to login with incorrect password. Exceptional events will require further investigation to determine an environment which may have led to an exception
- **Exceptions:** Events, which are unusual. Events may require closer monitoring. In some case the condition will resolve itself. For instance, unusual combinations of workloads as they are completed, normal operations will restore. In other cases, operations intervention will be required if the situation is repeated

Incident Management

An incident is an unplanned interruption to an IT service, or the reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service shall also be an incident.

Incident Management process provides guidelines that can be implemented by the banks for the management of incidents so that restoration of service operations as quickly as possible and to minimise adverse impact on business operations. The primary objective of the Incident Management procedures is to ensure best possible level of service quality and availability.

Problem Management

Problem Management process provides a framework, which can be implemented by banks to minimise the adverse impact of incidents on the IT Infrastructure and the business by identifying root cause, logging known errors, providing and communicating workarounds, finding permanent solutions, and preventing recurrence of incidents related to these errors. Problem Management increases stability and integrity of the infrastructure.

Problem Management process includes activities required to carry out the root causes of incidents and to determine the resolution to these underlying problems. Problem management procedures also include implementation of the resolution through Change Management procedures and Release Management procedures. This also includes appropriate turnaround and resolutions to incidents that cannot be resolved due to business cases, or technical short falls. Periodic trend analysis of the problems in respect of systems

or customer facing channels may be carried out and appropriate action taken.

Access Management

Access Management process provides the guidelines, which can be implemented by banks to limit access to IT services only to those individuals and applications that are duly authorised based on organisational policies and standards. Access Management enables the organisation to manage confidentiality, integrity of the organisation's data, IT infrastructure, and applications. *(Details have been provided in the "Information Security" chapter of the report.)*

KEY RECOMMENDATIONS

1. Bank's Board of Directors and Senior Management should oversee implementation of safe IT Operations environment. Policies and procedures, defined as a part of IT Operations, should support bank's goals and objectives, as well as statutory requirements.
2. Structure and functions in respect to service desk, IT operations, application and infrastructure management have been indicated for consideration. Service Desk needs to be the primary point of contact both for internal and external customers. IT Operations management is the function primarily responsible for day-to-day management and maintenance of an organisation's IT infrastructure, in order to ensure service delivery to the agreed level, as defined by Service Level Agreement. Infrastructure management function needs to be primarily responsible for providing technical expertise and overall management of the IT infrastructure.
3. Banks should analyse their IT Operation environment, including technology, human resources, and implemented processes to identify threats and vulnerabilities. They should conduct a periodic risk assessment.
4. As a part of risk identification and assessment, banks should identify events or activities that could disrupt operations or negatively affect reputation or earnings and assess compliance to the regulatory requirements.
5. Once banks have identified, analysed and categorised risks, they should define attributes for each risk component such as probability of occurrence and financial impact, among others. These, along with the business processes involved, should be used to prioritise risk mitigation actions and control framework.
6. Processes within IT Strategy provide guidance to identify, select and prioritise services need to be aligned to business requirements. IT Strategy as framework provides feedback to IT Operations on the services to be supported, their underlying business processes and prioritisation of these services. A well-defined IT Strategy framework will assist IT Operations in supporting IT services, as required by business and defined in SLAs.
7. Service Valuation is the mechanism that can be used by banks to quantify services, which are available to its customers (again, internal or external) and supported by IT operations in financial terms. Service Valuation will assist IT Operation Function to showcase the involvement of function in supporting the core business of banks. Service Valuation will have two components–provisioning value and service value potential.
8. Demand Management process needs to be used by banks to understand business processes IT operations supports to identify, analyse and codify patterns of business activities (PBA) to provide sufficient basis for capacity requirement.

9. Design phase of IT operations can be used by banks to manage changes in the business landscape. Components which should be considered when designing a new IT service or making a change to the existing IT service, include Business Processes, IT Services, Service Level Agreements, IT Infrastructure and IT Environment, among others.

10. Over the years, banks IT's infrastructure have grown and developed. There may not be a clear picture of all IT services currently being provided and consumers for each services. In order to establish an accurate IT landscape, it is recommended that an IT Service Catalogue is defined, produced and maintained. Service Catalogue can be considered as a repository that provides information on all IT services supported by the IT Operations framework. Service Catalogue Management process provides guidelines which can be used by banks to define and manage Service Catalogue, which provides consistent and accurate information on all IT services available to customers (internal or external). Service Catalogue Management process also ensures that service catalogue is available to users, who are approved to access it.

11. Banks need to institute Service Level Management process for planning, co-ordinating and drafting, agreeing, monitoring and reporting of service attributes used to measure the quality of service. The framework needs to include guidelines for ongoing review of service achievements to ensure that required and cost-justifiable service quality is maintained and gradually improved. Service Level Management framework, defined by banks, should also have guidelines defined for logging and management–including escalation of complaints and compliments. The critical aspects in this regard have been stipulated.

12. Capacity Management process is required to ensure that cost-justifiable IT capacity for IT services exists and matches the current- and future-agreed business requirements, as identified in Service Level Agreement. Banks adapting capacity management process should ensure that the framework encompass all areas of technology (hardware, software, human resource and facilities, among others).

13. Availability and reliability of IT services can directly influence customer satisfaction and a bank's reputation. Therefore, Availability Management is essential, to ensure that IT delivers the right level of service required by businesses to satisfy objectives. Availability Management process provides framework and guidelines that can be adapted by banks to ensure that the level of service availability is matched or exceeds the current and future requirements, as defined in Service Level Agreement.

14. Attributes that can be used by the banks for reporting availability of IT services include availability (in percentage), Mean Time between service incidents, Mean Time Between Failures and Mean Time to Repair–the formula for each of which have been defined.

15. When defining Availability targets for a business service, banks should consider identifying Vital Business Function (VBF). VBF represents critical business elements of processes supported by IT services.

16. The complex business demands require extensive skills and capabilities from IT to support business processes, therefore collaboration with service providers, value networks are an integral part of end-to-end business solution. Supplier Management process provides framework and guidelines which can be used by the banks to manage relationships with vendors, suppliers and contractors. The framework ensures that suppliers and the services they provide are managed to support IT service targets and business expectations.

17. Service Asset and Configuration Management framework can be used by banks to manage service assets and configuration items that supports business services. Implementation of Service Asset and Configuration Management framework has cost

and resources implications and therefore strategic discussions needs to be made about the priorities to be addresses. For instance banks can decide on initially focusing on the basic IT assets (hardware and software) and the services and assets that are business critical or covered by legal regulatory compliance.

18. Banks need to implement change management process for handling any changes in technology and processes to ensure that the changes are recorded, assessed, authorised, prioritised, planned, tested, implemented, documented and reviewed in a controlled manner and environment.

19. Operations phase as part of Service Management lifecycle is responsible for executing and performing processes that optimise the cost of the quality of services. As a part of the organization, it is responsible for enabling the business to meets its objectives. As part of technology, it is responsible for effective functioning of components that support business services. The aspects that banks need to consider: event, incident, problem and access management.