
PIT-201

Information Technology Process

Revision / Version	Date	Comments
1.0	08/10/2008	Nil
1.1	01/05/2009	Nil
2.0	30/11/2009	Nil
3.0	01/01/2013	Nil
3.1	16/07/2013	Nil
3.2	22/10/2013	Clause 3.6 / Associated Records Updated
3.3	05/12/2013	Addition of forms
4.0	14/05/2015	Addition of software management requirement
5.0	15/03/2016	Process Revamping
6.0	17/03/2017	Addition of Types of Changes
7.0	10/07/2020	ITSM (ISO/IEC 20000-1 Procedures added in IT SOP)

Information Technology Services Procedure

Table of Content

Contents

1.	Purpose:.....	5
2.	Scope:	5
3.	Definitions:.....	5
4.	Procedure and Policies.....	6
4.1	Processes for Competence Development:	6
4.1.1	Prior to Employment or Recruitment.....	6
4.1.2	During Employment	6
4.1.3	Post-employment or Termination and change of employment.....	7
4.2.	I.T. Services Operations Management.....	7
4.2.1	Call Logging and Escalation Process	8
4.2.2	Procedure for Request Fulfillment Management.....	8
4.2.3	Service Provider, Vendor and Partner Escalation	11
4.2.4	Incident Management	13
4.2.5	Problem Management.....	13
4.2.6	System Health Check and Audit	13
4.2.7	Server Maintenance.....	13
4.2.8	Network Resources Monitoring	14
4.2.9	Servers Resources Monitoring	15
4.2.10	Telephony Services Monitoring.....	15
4.2.11	Daily I.T. Checklists	15
4.2.12	I.T. Roster Management	16
4.2.13	I.T. Service Provider/ Vendor Management	16
4.3	Procedure for Service Management.....	16
4.3.1	New Service Induction.....	18
4.3.2	Change in Service.....	21
4.3.3	Service Retirement	22
4.3.4	Procedure RACI Matrix	23
4.4	Procedure for Services Performance Measurement	24
4.4.1	Performance Monitoring Procedure Description	24
4.4.2	Responsibilities	24
4.5	Service Reporting Policy.....	24
4.5.1	Service Reporting Frequency and Methodology	27
4.6	Configuration Management	36
4.6.1	Planning.....	37

Information Technology Services Procedure

4.6.2	Identification	37
4.6.3	Controlling.....	38
4.6.4	Services Configuration	38
4.6.5	Server, Network and VoIP Systems Configuration	38
4.6.6	End-User Configuration	39
4.7	Procedure for Demand Management.....	40
4.7.1	Establish Demand Management Framework	40
4.7.2	Evaluate Demand Requirements	40
4.7.3	Gather Demand and Usage Data	41
4.7.4	Identify Patterns of Business Activity and User Profiles	41
4.7.5	Develop Demand Forecast	41
4.7.6	Plan and Implement Demand Management Initiatives	41
4.7.7	Monitor, Manage and Report Demand Management	41
4.8	Change Management.....	42
4.8.1	Change Management Obligation	42
4.8.3	Change Management Request for Movement of Fixed Assets	43
4.8.4	Change Management Review	43
4.9	Asset Management.....	43
4.9.1	I.T. Acquisition / Requisition Process.....	43
4.9.2	Equipment Issuance	44
4.9.3	I.T. Inventory Management	44
4.9.4	Secure Disposal and Reuse of I.T Equipment	44
4.10	Access Rights Management	45
4.10.1	Internet/ Wireless Access	46
4.10.2	Internal Network	46
4.10.3	Printer/Scanner.....	46
4.10.4	File Server Access	47
4.11	Access Rights Review	47
4.12	Information Security Management	47
4.12.1	Event Logging	48
4.12.2	Network Security & Management.....	48
4.12	Email Transmission	48
4.12.4	User Account Management.....	49
4.12.5	Anti-Malicious	49
4.12.6	Drive Encryption	50
4.12.7	Secure Communication and Infrastructure	50

Information Technology Services Procedure

4.12.8 Patch & Technical Vulnerability Management	51
4.12.9 Resource Usage Logs	51
4.13 Capacity Management	51
4.13.1 Forecast Future Capacity Requirements	52
4.13.2 Plan to Meet Requirements (Capacity Planning)	53
4.13.3 Current and Forecast Demand for Services	53
4.13.4 Service and Resource Summary and Recommendations	54
4.13.5 Monitor, Analyze and Report on Resource Usage	54
4.13.6 Tune to Make Best Use of Resources	55
4.13.7 Component Capacity Management	55
4.13.8 Service Capacity Management	55
4.13.9 Business Capacity Management	55
4.15.1 Service continuity and availability requirements	56
4.15.2 Service continuity and availability plan	57
4.15.3 Service continuity and availability monitoring and testing	57
4 Associated Policies/Processes/Guidelines:	58
5 Associated Records:	59

Information Technology Services Procedure

1. Purpose:

The purpose of this document is to describe the Information Security, Network, Systems, Voice Infrastructure and Computer operating procedures for SYBRID. It will describe the business requirements for Network, Systems, Voice Infrastructure and support. Roles and Responsibilities at different level are also identified in the document. Communication channels for assistance are also elaborated.

Operating procedures for Anti Malicious and Mobile Code, User Account Management, Security Management, Management of Removable Computer Media and Security Configuration Guide for Operating System and Software will also be enclosed in this document.

2. Scope:

The requirements of this procedure apply to all IT processes to meet the compliances of ISMS to regulate a hi-tech and fully controlled environment for IT service delivery with the following practices.

- I.T. Services Operations Management.
- Configuration Management.
- Change Management.
- Asset Management.
- Access Rights Management.
- Information Security Management.
- Capacity Management.
- Project Management.
- IT Disaster Recovery & Business Continuity Procedure

3. Definitions:

Abbreviations/Terms	Description
IP	Internet Protocol
FTP	File Transfer protocol
LAN	Local Area Network
ISP	Internet Service Provider
SLA	Service Level Agreement
OLA	Operational Level Agreement
BU	Business Unit
CS	Customer Services
MD	Medical Division
TS	Telecom Services
BD	Business Development

Information Technology Services Procedure

NMS	Network Management System
UAN	Universal Access Number
TFN	Toll Free Number

4. Procedure and Policies

4.1 Processes for Competence Development:

- Sybrid IT Team must be provided legitimate training regarding the Policies, procedures, running systems, services and information security compliances at the time of hiring. These records will be maintained in **RIT-224 IT Resource Training Record**.
- Access to any required information to any Sybrid IT Team member must be on the basis of completion of training.
- Manager/A.M. IT must ensure that initial training is completed and successful prior to setting up the particular IT resource operational in LIVE environment.
- SYBRID ITS Department determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the Quality & information technology services management system. This process has 3 levels of management
 - a) Prior to employment
 - b) During employment
 - c) Post-employment or Termination and change of employment

4.1.1 Prior to Employment or Recruitment

This is regarding the hiring of new employee in ITS Department and this will be taken care as per HR Department policy.

4.1.2 During Employment

4.1.2.1 SUBSEQUENT TRAINING / OJT

Subsequent training, including on-the-job training ("OJT") is performed to ensure each employee is knowledgeable in their job function and their role within the company.

The Employee Training Need Assessment Sheet lists applicable task-specific requirements for some positions; for employees hired in these positions, the Line Manager will update this matrix as training is conducted for these tasks.

On the Employee Training Need Assessment Sheet, an employee is considered qualified if the task is marked off as completed; the employee may train others if this is indicated.

Prior to qualification, an employee's supervisors or line managers are responsible for that employee's work.

Other training is recorded on individual employee training records. Such records should indicate the following:

- a) Type of training
- b) Method of training
- c) Duration of training
- d) Date of completion

Information Technology Services Procedure

- e) Location of training
- f) The name of the instructor or individual who conducted the training

Personnel undergoing third party training and receiving a certificate of training by the training provider may retain this certificate as a training record in lieu of an employee training record. All training records are to be maintained in the employee training records.

4.1.2.2 Training Evaluation

Management periodically reviews and re-certifies employees for operations where recertification is required or beneficial. Annual personnel evaluations are performed to assess effectiveness of training. Employee evaluations shall include goals for continual improvement and KPI's of the employee's competency and abilities, as well as their growth within the company, as applicable.

Where appropriate, some training programs will include a test or other means of verifying the effectiveness of training. In such cases, work instructions will define the minimum passing grade, and actions to be taken when an employee does not pass.

If problems, weaknesses or concerns are discovered during an evaluation or otherwise reported for any other reason (including customer complaints), a CAR (Corrective Action Request) Log form shall be completed to identify weaknesses and develop a plan of improvement for that employee.

4.1.2.3 Annual Performance Evaluation and Promotion

Quarterly Performance records need to be maintained for each employee by line managers which is based on JDs, Goals and KPIs.

Employee's performance is evaluated as per HR Policy.

It is ITS's goal to ensure maximum opportunity for promotion from within, consistent with the commitment to organizational needs, equal opportunity and applicable contractual agreements. It is recognized that a promotion may occur in the following cases:

- a) A reclassification of the individual's existing position as a result of the individual performing duties at a higher degree of responsibility and complexity than the current classification calls for. This requires an audit of the position through the job evaluation process.
- b) The filling of an existing higher level vacancy by a promotable individual at a lower classification.

4.1.3 Post-employment or Termination and change of employment

This is regarding the resignation and termination of employee in ITS Department and this will be taken care as per HR Department policy.

4.2. I.T. Services Operations Management

Sybrid IT Team is responsible to provide all the IT enabled services and responsible to provide these services with a combination of in house and third party services to meet the business requirements for internal and external customers. Following IT Services will be included in scope of work.

- Networks Services
- Telephony Services
- Internal Network

Information Technology Services Procedure

- Infrastructure & Applications Services
- Service Desk

4.2.1 Call Logging and Escalation Process

All the incidents, problems, service requests and queries will be logged into **Sybrid IT Service desk** (<http://servicedesk.int.sybrid.com> for KHI or <http://helpdesk.sybts.local/> for ISB) as per the following procedure.

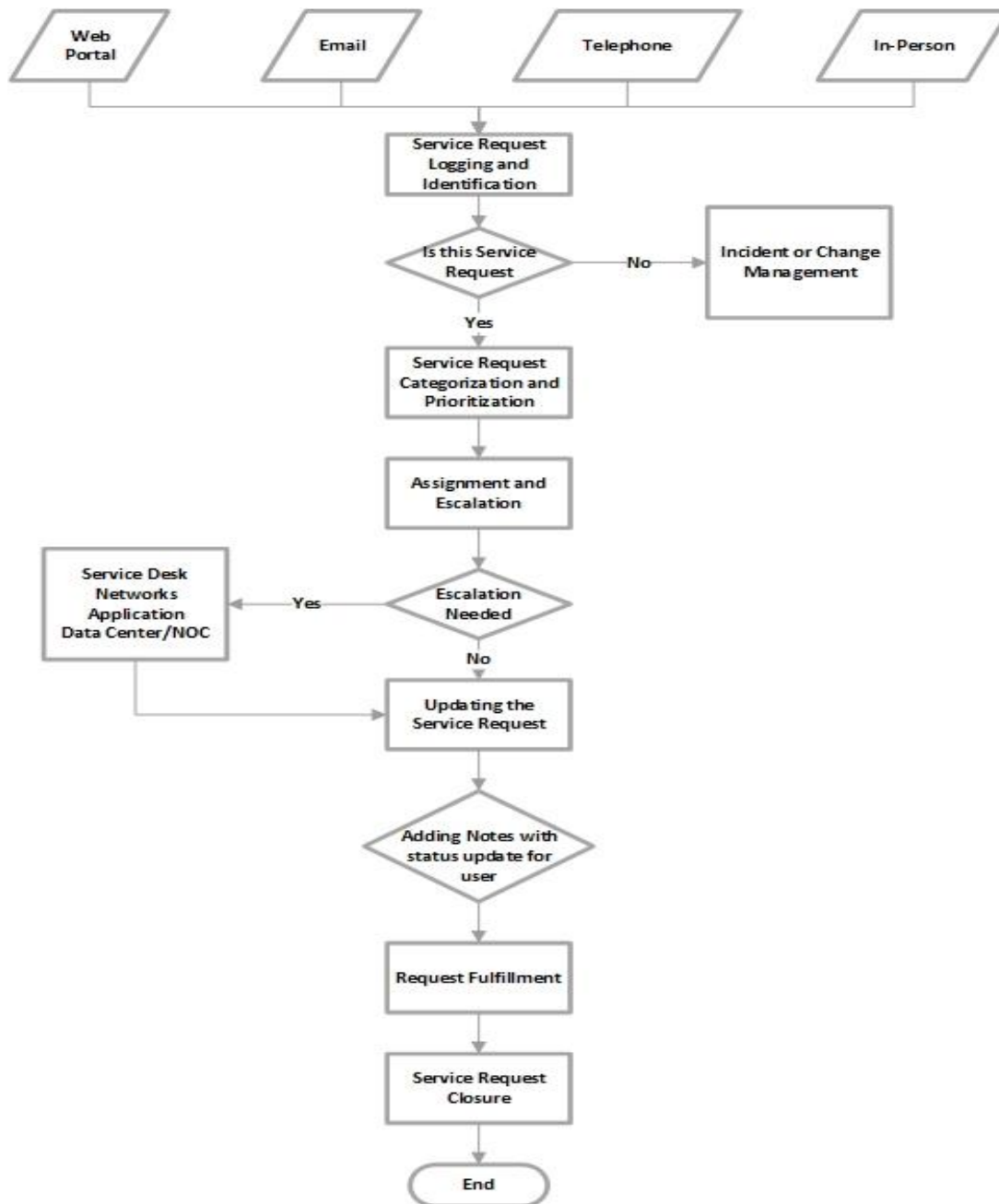
- Customer will report all its tickets to IT Support via **Sybrid IT Service desk** or Email (support@sybrid.com/Support@sybridts.com) or by calling 3000/6004 extension.
 - System Support Engineer will log ticket complaint in **Sybrid IT Ticketing system** and the ticketing system generates a unique ticket ID that captures the event, event source, initial event severity and event Priority
 - IT Department uses this unique ticket ID for formal communication with customer as a reference number.
 - System Support Engineer will try to resolve it over the phone, if not able to resolve he/she will visit the individual on his/her seat.
 - System Support Engineer will escalate this issue to Systems Engineer/Administrator if any backend configuration changes are required.
 - Systems Engineer will resolve it by making changes on backend configuration. If he is unable to resolve it and requires some major configuration change he/she will escalate it to Systems Administrator.
 - If Systems Administrator is unable to resolve and requires some strategic/Design level change he will escalate it to AM-IT/ Manager IT.
 - System Support Engineer will update the ticket on **Sybrid IT Service desk**
 - **Sybrid IT Service desk** Ticket will also be updated by Support engineer even if the problem is resolved over the phone and ticket will be closed after client approval through helpdesk.
 - System, Network and Voice Support Engineers are available in all shifts and will respond to all the emails on support@sybrid.com/Support@sybridts.com and calls on extension 3000/6004.
 - In case of any escalation is required he will perform it as per defined process.
 - IT Team Lead will ensure that all emails and extension calls are entertained properly as per agreed SLA/OLA.

4.2.2 Procedure for Request Fulfillment Management

This process needed to fulfill service request will vary depending on exactly what is being requested. This can be communicated directly by users, through the Service Desk, through an interface from Service Request Management tools, by calling the helpline or by visiting ITS service Desk.

The process of request fulfillment management majorly delivered by the Service Desk function. Service Desk is the single point of contact between the ITS and customers.

Information Technology Services Procedure



Procedure Flowchart

Information Technology Services Procedure

Procedure Flowchart Description

Service Request can triggered from one of the followings Channels:

Web Portal: <http://servicedesk:8080/>

Email: User can submit request by sending an email to support@sybrid.com

Telephone: User can call on **3000** and Service Desk representative will log the incident on behalf of user.

In-Person: User can visit Service Desk area and Service Desk representative will log the service requests and provide the support to the user.

4.2.2.1 Service Request Logging and Identification

This step is used for logging the service request and identification of service request either this is service request or part of incident / change.

Service request logged by using the given channels (Web Portal, Email, Telephone and In-Person).

Service Desk representative will log the service request whenever received the requests by call or in-person.

Service Desk representative will perform the identification for the service requests those are created by using portal or email, these are either service requests or part of incident / change.

4.2.2.2 Service Request Categorization and Prioritization

This step is used by the service desk to check and set Service category along with sub category and the priority of requests based on criteria.

Service Desk representative will check and set the Service Category and Subcategory for all the reported service requests based on Service Catalog.

Service Desk representative will check and reset the priority of the service requests as per criteria of service request priority.

4.2.2.3 Assignment and Escalation of Service Request

This step is used by Service Desk representative and other support representative for assignment and escalation to other level within ITS wherever required.

Service Desk representative will review the request and if it can be fulfilled on initial level then assigned to his/herself. Like; password reset request.

If the service request cannot fulfill on level 1 then Service Desk representative will either escalate the service request within Service Desk team or to other ITS teams (Network / Application / Data Center (NOC) with initial collected details.

This escalation or assignment should be done as per Service Catalog of ITS.

4.2.2.4 Updating the Service Request

This is for adding updates for all service request.

Always update the request record with actions carried out, even if it is only the fact that the user was telephoned without success. This shows activity on the request that is useful to the Service Desk if the user calls for an update.

Information Technology Services Procedure

Make sure the request is set to the correct status at all times, including when waiting for feedback from the user.

Inform the user with actual status even in case supplier management is involved for fulfillment of request.

4.2.2.5 Request Fulfillment

This is when the support person confirms that the user's service request has fulfilled as per requirement.

Once the support provided to the user for service request, the owner of service request will confirm from user before marking resolve/ close the Service Request also update the same in service request. Service request owner will make sure to update the records in the related to CIs in CMDB for all the service requests wherever required.

4.2.2.6 Service Request Closure

At this point, the service request is considered as resolved / closed and the service request process ends.

Service Request owner will mark the service requests as resolved / closed now.

Service request owner will use Resolution Standard template if available in Knowledgebase.

In case standard resolution not available in knowledgebase, then note down the performed steps during request fulfillment and update as new fulfillment in knowledgebase. So that it might be helpful for ITS in future.

4.2.3 Service Provider, Vendor and Partner Escalation

Sybrid IT will perform escalation to service providers, vendors and partners for third party services in case if required as per the following details.

In case of any Service Downtime, it must be calculated on the basis of **RIT-209 IT Uptime Report** and a rebate shall be claimed to the service provider as per rebate criteria mentioned in Contract.

Service	Service Provider	Method	Email
Internet/ Data Connectivity	Cyber Internet Services	* By Calling CN NOC 5654 * Email on provided addresses	helpdesk@cyber.net.pk
			noc_khi@cyber.net.pk
			tac-south@Cyber.net.pk
Telephony Services CS & TS - (UPL, Haier, OPTP, CAP, IMC & Interwood)	Multinet	* By Calling MN NOC 111 247 000 *Email on provided addresses	ots@multinet.com.pk
			fll.noc@multinet.com.pk
			inam.haider@multinet.com.pk

Information Technology Services Procedure

Telephony Systems & Services CS - MCD, Colgate and 'CYBERNET)	Cyber Internet Services	* By Calling CN NOC 5940 * Email on provided addresses	ngn-noc@cyber.net.pk
---	-------------------------	---	--

Telephony Services MD (Back Office, Front Office)	InPhonex	*Open a ticket on InPhonex Portal	www.inphonex.com
Telephony Services MD (Systec)	Alcazar Network	*Email on provided address	support@alcazartnetworks.com
Sybrid Karachi PBX- External	Cyber Internet Services	* By Calling CN NOC 5940 * Email on provided addresses	ngn-noc@cyber.net.pk
Sybrid Islamabad Internet Service	Multinet Private Limited	* By Calling MN NOC 111 247 000 * Email on provided addresses	OTS@multinet.com.pk fll.noc@multinet.com support@multinet.com
Sybrid Islamabad Internet Service	NayaTel Internet Services	* By Calling NT NOC 111 114 444 * Email on provided addresses	support@nayatel.com

Information Technology Services Procedure

4.2.4 Incident Management

- Services downtime or serious performance degradation and information security risk/breach shall be considered as an Incident and shall be managed according to incident classification in terms of its severity and impact on IT operations in line with the Incident Reporting and Response Procedures.
- Incidents affecting service impact and security shall be reported through appropriate escalation process to Sybrid IT (Refer to IT Call logging & Escalation process).
- Root Cause Analysis will be carried out for every incident which provides a substantial service impact and security risk.
- An incident report shall be created; types, volume and costs of the incidents and malfunctions to be quantified and monitored and maintained in **RIT-203 Service Incident Report** and share it with relevant stake holders within next 24 hours.
- Any security incident or weakness must be maintained on **RISM-902** by following the Security incident/weakness reporting procedure.

4.2.5 Problem Management

- Re-occurrence of incidents on similar pattern will be considered in Problem Management.
- Root Cause Analysis will be carried out for every problem which provides a substantial business impact.
- Sybrid IT Team will explore best possible solution and perform rectification in order to give the permanent fix to problems.
- All the trends and reporting shall be maintained on Sybrid IT Service desk
- Sybrid IT will ensure all the problems are managed as per agreed SLAs/OLAs.
- After the problems are resolved System Support Engineer will close the ticket at helpdesk system.

4.2.6 System Health Check and Audit

- System, Network or VoIP Support Engineers are responsible to perform weekly health check and Audit to review system performance and logs.
- If System, Network or VoIP Support Engineers found any unwanted or personal data on shared system, software, malware or any malicious content on employee's system incident should be raised by following security incident & weakness reporting mechanism.
- All the system audit checks will be maintained in **RIT-213 System Audit Report**.
- All the System health checks will be maintained in **RIT-212 System Health Check Report**.

4.2.7 Server Maintenance

- System, Network or VoIP Engineers are responsible to perform bi-monthly maintenance and review system performance and event logs of servers.

Information Technology Services Procedure

- Maintenance will always be planned and informed to senior Management at least before 24 hours. This intimation will be circulated through notification on ERP Portal.
- In case of any urgent maintenance IT Team will inform all HODs via notification on ERP Portal just before the activity.
- Any vulnerability observed shall be noted and highlighted to the concerns prior to performing any corrective actions.
- All the system maintenance activity will be updated in **RIT-211 Maintenance Report**.

4.2.8 Network Resources Monitoring

- System, Networks or VoIP Support Engineers are responsible to monitor Network resources (Bandwidth, Broadcast, Port Utilization and other traffic) using Solar winds NMS. (<http://192.168.61.198/Orion/Login.aspx> for KHI & <http://isb-nms-d001/Orion/Login.aspx> for ISB) with their provided credentials by using **GIT-204 Client end Configuration** for Karachi & **GIT-304 Client End Configuration Guideline-ISB** for Islamabad site.
- Specified thresholds (75%) are defined for respective services and devices in monitoring system and in case of its breach some alarms are generated.
- In case of any alarm is generated System, Networks or VoIP Support Engineer will highlight it to Systems Engineer and Systems, Networks or VoIP Administrator for further diagnosis & troubleshooting.
- Any unusual activity over internet will be reported to specific line manager and ISM for further disciplinary action.
- In case any unusual behavior of any service or device is observed, Systems Engineer will notify all stakeholders and perform required maintenance.
- Daily Monitoring activity will be updated in **RIT-222 Daily Network Monitoring Sheet** by System, Networks or VoIP Support Engineer and will be updated on ERP portal at day end.

Information Technology Services Procedure

4.2.9 Servers Resources Monitoring

- System, Networks or VoIP Support Engineers are responsible to monitor Server resources (RAM, CPU, Storage, Network and Power utilization) using VMware Server Monitoring for Karachi servers refer **GIT-204 Client end Configuration** and **GIT-304 Client End Configuration Guideline-ISB** for Islamabad servers with their provided credentials.
- Specified thresholds (75%) are defined for respective services and devices in monitoring system and in case of its breach some alarms are generated.
- In case of any alarm is generated System Support Engineer will highlight it to Systems, Networks or VoIP Engineer/Administrator for further diagnosis and troubleshooting.
- Any unusual activity with data held on servers will be reported to specific line manager and QA for further disciplinary action.
- In case any unusual behavior of any service or device is observed, Systems Engineer will notify all stakeholders and perform required maintenance.
- Daily Monitoring activity will be updated in **RIT-223 Daily Server Monitoring Sheet** by System, Networks or VoIP Support Engineer and will be updated on ERP portal at day end.

4.2.10 Telephony Services Monitoring

- System, Networks or VoIP Support Engineers are responsible to monitor Telephony Services by testing UAN/TFN and backend numbers.
- Any vulnerability observed should be immediately highlighted to concerned service provider/service owner for resolution.
- In case any unusual behavior of any service or device is observed, Systems Engineer will notify all stakeholders and perform required maintenance.
- Daily Monitoring activity will be updated in **RIT-221 Daily UAN Audit Sheet** by System, Networks or VoIP Support Engineer and will be updated on ERP portal at day end.

4.2.11 Daily I.T. Checklists

- System, Networks or VoIP Support Engineers are responsible to perform daily floor checklist prior to shift start.
- Daily Floor checklist shall be updated on ERP Portal **RIT-225 Daily IT Floor Checklist-Sybrid MD**, **RIT-226 Daily IT Floor Checklist-Sybrid CS** and **RIT-229 Daily IT Floor Checklist-Sybrid TS**.
- Systems Engineers/Administrators are responsible to perform daily servers, networks and telephony checklists.
- In case any unusual behavior of any service or device is observed, Systems Engineer/Administrator will notify all stakeholders and perform required maintenance.

Information Technology Services Procedure

4.2.12 I.T. Roster Management

- Sybrid IT plan roster for IT Team according to work load with 24/7 availability.
- On Weekdays (Monday to Friday) all engineers were available according to their shifts for Karachi IT Team whereas for Sybrid Islamabad roster will be managed for all seven days with 1 off day for every engineer on any day of the week.
- On weekend (Saturday & Sunday) 1 off for all engineers according to roster.
- Sybrid IT Roster is formed monthly by Team Lead and reviewed by Manager I.T. and A.M.
- I.T. which is shared to all stake holders via email.

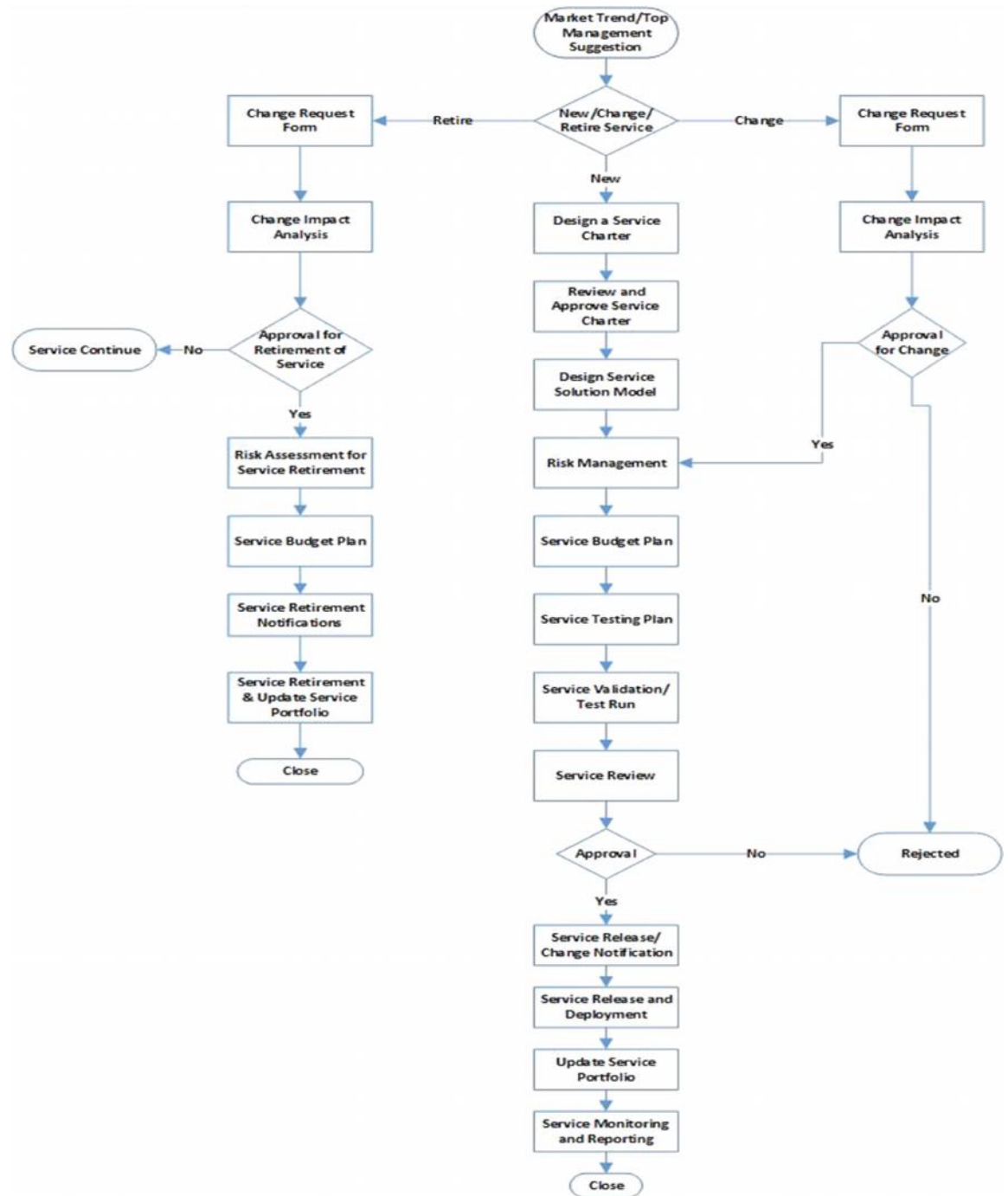
4.2.13 I.T. Service Provider/ Vendor Management

- Sybrid IT team must ensure proper screening of Vendors/ Service providers and partners considering the Type of services meeting the business requirements, Cost of services, Quality of Services & information security risk.
- Sybrid IT Team must ensure SLA with the service provider to ensure all the necessary business and information security requirements.
- Any SLA between Sybrid IT and service provider must include the following points.
 - Service Provider Call Logging process & Escalation Matrix with TAT.
 - Mutually agreed pricing, billing and rebate structure.
 - Dispute resolution between two parties.
 - Information Security & Access to information.

4.3 Procedure for Service Management

Sybrid IT Team will review the process applies to the phases of the lifecycle of any new service and changed in service. The process of service's lifecycle, which includes new and change services, service demand, service test, service release and the retirement of services if required.

Information Technology Services Procedure



Information Technology Services Procedure

Procedure Flowchart Description

There are three scenarios related to Service Management:

New Service Induction

Change in Service

Service Retirement

4.3.1 New Service Induction

In case of new service induction here is the process details

4.3.1.1 CRF

At first needs are articulated to design as service charter based on the customer requirements which Includes a high-level description of a new service and the approach to build that service. In particular, the Service Charter outlines the deliverables to be created during the service implementation project, the required resources, and an initial project schedule.

4.3.1.2 Review and Approve CRF

Once the Service Charter is designed then before proceeding further on this, approvals are required from interested parties (Stakeholders).

4.3.1.3 Design Service Solution Model

A Service solution Model is designed which includes a high-level description of a service and the components required to deliver that service. The main purpose of service solution models is to facilitate an understanding of what service components, assets and other resources are necessary to create the service, including their interactions. Service solution models are a valuable tool for understanding the impact of proposed new services on other services at an early stage.

4.3.1.4 Risk Management

Risks include anything that could impact the strategic objectives and operational readiness of the organization the governance body directs and controls. Risk surveillance, detection, evaluation and response should be imbedded into the IT governance system. A risk register should be maintained and appropriate personnel assigned by the governance body to manage risk issues within the organization for new service induction, change in service or retirement of any service.

4.3.1.5 Service Budget Plan

During this step we will determine about the overall budget planning for the introduction of new service of change in a service.

4.3.1.6 Service Testing Plan

At this stage the testing plan of any new or changed service will be determined based on it service validation and testing will be performed.

Information Technology Services Procedure

4.3.1.7 Service Validation /Test Run

Service Validation/Test Run is the process used for actively maintaining test environments, and to ensure that the developed releases meet the customer's expectation. This is to check either the service is as per required needs and meeting the needs as defined in Service Charter.

4.3.1.8 Service Review

This is to check service is as per required needs and meeting the needs as defined in Service Charter based on service test run and validation as above at **7.2.1.8**. Based on reviewing the Service either approval was provided to proceed for new or change service release or rejected.

4.3.1.9 Service Release Notification

During this process communication for release will be started to the interested parties (stakeholders), and there can be single or multiple communications based on approach of release plan.

4.3.1.10 Service Release and Deployment

ITS team will ensure that releases are deployed into production efficiently and effectively. Here, the "Release" means the development of a newer version of a service or component, whereas the "Deployment" means the process of integrating it into the production environment. The part of Release Management is tightly bound with Change Management and Configuration Management to ensure proper evaluation, tracking and record keeping of all new and old releases. Further, the deployment section also has to work together with incident management for a small period of time when new releases are just deployed to production.

4.3.1.11 Update Service Portfolio

Regarding new or changed service needs to update the Service Portfolio accordingly with all the aspects as agreed with customers and communicate to the customers as well.

4.3.1.12 Service Monitoring and Reporting

This includes the following:

- i. Governance of Processes Operated by Other Parties

Most processes or parts of processes shall be operated by the internal IT teams only with the exception of provision and maintenance of cloud infrastructure (provided and maintained by Cloud Services Department).

- ii. Interfaces between Service Management Processes

The processes of Service Management are closely related to each other, with outputs from one being inputs to another. There is no overall process model in existence as part of Good Practice, but the following sections give an indication of the ways in which the processes interact within ITS department.

Information Technology Services Procedure

A. Service Desk Function

The Service Desk acts as the focal point for a number of processes, particularly Incident and Request, Problem, Change and Configuration Management. The Service Desk system supports these processes.

B. Incident Management

Multiple incidents logged at the Service Desk may result in a Problem being raised. The Incident Management function will use information from Change and Configuration Management to assess and resolve incidents, and such resolution may require a change to be implemented via Change Management.

C. Problem Management

Problems are largely raised from incidents and may also have a significant relationship with Availability Management in identifying the root cause of a lack of system availability.

D. Change Management

The Change Management function relies upon the data in the Configuration Management Database to assess the impact of changes, just as Configuration Management relies upon Change Management to keep its records up to date. Change Management also has a strong link to Release and Deployment Management and will need to liaise with the Service Desk to keep its staff aware of changes that may impact service.

E. Configuration Management

Configuration Management underpins many of the other processes including Incident, Problem, Change, Capacity and Availability Management by providing accurate information about installed hardware, software and documentation.

F. Supplier Management

Efficient management of suppliers is vital for effective Service Level Management and the achievement of SLA targets. It is also important to Budgeting and Accounting in providing information to allow accurate budgeting. Various other processes provide input to Supplier Management, including Incident, Problem, Change and Configuration Management.

G. Service Level Management & Reporting

Defining and achieving service levels relies heavily upon many of the other processes, particularly Capacity, Availability, Problem and Incident Management.

H. Business Relationship Management

This process requires accurate information from Service Level Management and Reporting and many of the other processes contribute to encouraging a good relationship with the business.

I. Budgeting and Accounting for IT Services

Information Technology Services Procedure

The Capacity Planning process provides information regarding upcoming upgrades to Budgeting and Accounting and an interface with Service Level Management allows the cost implications of different Service Levels to be explored.

J. Service Management Planning

Service Management Planning covers all of the processes of Service Management and benefits from feedback from each of them via the Service Improvement process.

K. Release and Deployment Management

Release and Deployment Management has a strong interface with Configuration and Change Management as it uses and updates configuration data and makes use of the Change Management process to achieve its aims.

L. Capacity Management

This process has inputs from Service Level Management and Configuration Management amongst others and provides information to Budgeting and Accounting and Change Management.

M. IT Service Continuity and Availability Management

Availability Management has an interface with both Incident and Problem Management as sources of issues and to Service Level Management for the setting of objectives and reporting against them.

The IT Service Continuity Plan must be kept up to date and this is achieved via the Change Management process. Many of the other processes provide input to the Plan such as Capacity, Availability and Budgeting and Accounting.

N. Human Resources

This process ensures that the skills to deliver all of the other processes are in place and so underpins the process model in general.

O. Information Security Management

Security will be considered as part of a new or changed service and when assessing changes. Security requirements will also be reflected in SLAs.

4.3.2 Change in Service

In case of changing in existing service here is the process details

4.3.2.1 Market Trend & Top Management Suggestion

The process initiated while received the request based on the market trends or by top management suggestion for changing/modification in existing service.

4.3.2.2 Change Request Form

Change request form will be submitted with all the details (Purpose, rollback plan, service etc.), for a change in any existing service for review to CAB.

Information Technology Services Procedure

4.3.2.3 Change Impact Analysis

During this process needs to provide the full details regarding the impact of this change in service and value, pre and post analysis of change.

Based on this Change Impact Analysis CAB will take decision either to approve or disapprove the change.

In case of approval follow the process from “**points 7.2.1.5 until 7.2.1.13** from above **7.2.1. New Service Induction.**

4.3.3 Service Retirement

In case of retiring the existing service, here is the process details

4.3.3.1 Market Trend & Top Management Suggestion

The process initiated while received the request based on the market trends or by top management suggestion for retiring the existing service.

4.3.3.2 Change Request Form

Change request form will be submitted with all the details (Purpose, rollback plan, service etc.), for retiring the existing service for review to CAB.

4.3.3.3 Change Impact Analysis

During this process needs to provide the full details regarding the impact of this retirement of service related change and value return, pre and post analysis of change.

Based on this Change Impact Analysis CAB will take decision either to approve for this service retirement or disapprove to continue the service as it is.

4.3.3.4 Risk Assessment for Retirement of Service

Risks include anything that could impact the strategic objectives and operational readiness of the organization the governance body directs and controls. Risk surveillance, detection, evaluation and response should be imbedded into the IT governance system. A risk register should be maintained and appropriate personnel assigned by the governance body to manage risk issues within the organization for retirement of any service.

a. Service Budget Plan

During this step we will determine about the overall budget planning for the removal/retirement of service.

b. Service Retirement Notification

During this process, communication for removal/retirement of service will be started to the interested parties (stakeholders), with retirement timelines and multiple reminders included in it.

c. Service Retirement & Update Service Portfolio

Service will be retired and the Service Portfolio updated accordingly with all the aspects as agreed with customers and communicate to the customers as well

Information Technology Services Procedure

ITS-SOP v7.0

4.3.4 Procedure RACI Matrix

RACI for New Service					
S#	Activity Name	MR	Project Manager	Service Owner	Head of ITSM Steering Team
1	Service Charter	I	AR	C	I
2	Service Solution Model	I	I	ARC	I
3	Risk Management (Service Capacity Management)	C	I	AR	I
4	Risk Management (Service Capability Management)	C	I	AR	I
5	Service Budget Plan	I	AR	I	C
6	Service Testing Plan	C	I	AR	I
7	Service Validation	I	I	ARC	I
8	Service Review and Approval	I	I	C	AR
9	Service Release Notification	C	I	AR	I
10	Service Release and Deployment	I	I	ARC	I
11	Update Service Portfolio	AR	I	C	I

RACI for Change in Service					
S#	Activity Name	MR	Project Manager	Service Owner	Head of ITSM Steering Team
1	Change Request Form	ARC	I	RC	I
2	Change Impact Analysis	I	A	RC	R
3	Risk Management (Service Capacity Management)	C	I	AR	I
4	Risk Management (Service Capability Management)	C	I	AR	I
5	Service Budget Plan	I	AR	I	C
6	Service Testing Plan	C	I	AR	I
7	Service Validation	I	I	ARC	I
8	Service Review and Approval	I	I	C	AR
9	Service Change Notification	C	I	AR	I
10	Service Release and Deployment	I	I	ARC	I
11	Update Service Portfolio	AR	I	C	I

RACI for Retiring the Service					
S#	Activity Name	MR	Project Manager	Service Owner	Head of ITSM Steering Team
1	Change Request Form	ARC	I	RC	I
2	Change Impact Analysis and Approval	I	A	RC	R
3	Risk Management (Service Capacity Management)	C	I	AR	I
4	Risk Management (Service Capability Management)	C	I	AR	I
5	Service Budget Plan	I	AR	I	C
6	Service Retiring Notification Plan	C	I	AR	I
7	Service Retiring Notifications	C	I	AR	I

Information Technology Services Procedure

8	Service Retirement	C	I	AR	I
9	Update Service Portfolio	AR	I	C	I

4.4 Procedure for Services Performance Measurement

The ITSM team is responsible for measuring and monitoring the performance of ITS department at Sybrid services management system at relevant planned interval.

4.4.1 Performance Monitoring Procedure Description

ITS steering team evaluates the services performance and the effectiveness of the services delivered.

Following parameters are analyzed to evaluate the performance and effectiveness of the services management system:

- a) Availability;
- b) Endpoint Protection;
- c) SLA Management;
- d) Customer Satisfaction;
- e) Access Control Security;
- f) Objectives Measurement (Annual);
- g) Review and Reporting;
- h) Supplier Management;
- i) Backup and Recovery;
- j) Application Management.

Top management evaluates the performance on every management review meeting using performance monitoring sheet and its trend analysis.

4.4.2 Responsibilities

ITSM Steering team is responsible to manage the overall service performance of SMS which includes the following roles:

Head of ITSM Steering Team
Management Representative
Project Manager
Document Controller
Service Owners

4.5 Service Reporting Policy

Data shall be collected as per parameters and report shall be generated at the defined frequency which can be, hourly, daily, weekly, monthly or quarterly.

Information Technology Services Procedure

Data Analysis shall be conducted by the service owners as per service level requirements (SLRs) and service level agreements (SLAs).

Service report shall be sent to the relevant stakeholders by the service owners at predefined frequency.

Information Technology Services Procedure



Information Technology Services Procedure

Process can be triggered with the delivery of service and breakdown occurrence in the services.

Consider the agreed level of the services to identify the parameters of the service reporting.

Data is collected as per parameters at the defined frequency which can be, hourly, daily, weekly, monthly or quarterly.

Data Analysis conducted by the service owners as per service level requirements (SLRs) and service level agreements (SLAs).

Report is generated by the service owner as per the measurements based on SLAs and service parameters to present the true and concise picture of the service.

Service report is sent to the relevant stakeholders by the service owners at predefined frequency.

The reported service also feeds in the entire service performance log.

4.5.1 Service Reporting Frequency and Methodology

Service report shall be sent by the service owners via email using service report template as an attachment at monthly frequency, within the first five (5) working days of each month.

Below described is the methodology of all internal service reporting within ITS department at Sybrid to:

- **Chief Solution Officer (CSO)**
- **Management Representative (MR)**

Whereas business strategy and performance related reporting will be followed as per Procedure for Service Management and Service Performance Log:

Information Technology Services Procedure

S#	Report Name	Service Owner	Reporting Parameters		Reporting Parameters Reference
1	Authentication Services	NOC infra Team	Availability:	24/7	Attached Relevant Parameters in Service Report
			Endpoint Protection:	Servers 100%, Workstation 90%	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	96%	
			Backup and Recovery (RPO):	99.99%	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

2	End User Computing	Manager Service Desk	Availability:	Business Hours (8am to 8pm - Monday to Saturday)	Attached Relevant Parameters in Service Report
			Endpoint Protection:	Workstation 90%	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	NA (It applies through Authentication Services)	
			Backup and Recovery (RPO):	NA (No backup and recovery services are provided to desktops as per policy)	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

3	Operating System & Software Support	Manager Service Desk	Availability:	Business Hours (8am to 8pm - Monday to Saturday)	Attached Relevant Parameters in Service Report
			Endpoint Protection:	Workstation 90%	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	NA (It applies through Authentication Services)	
			Backup and Recovery (RPO):	NA (No backup and recovery services are provided to desktops as per policy)	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

4	Server and Storage	NOC infra Team			Attached Relevant Parameters in Service Report
			Availability:	24/7	
			Endpoint Protection:	Servers 100%	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	96%	
			Backup and Recovery (RPO):	99.99%	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

5	Network Access and Control	NOC infra Team			Attached Relevant Parameters in Service Report
			Availability:	24/7	
			Endpoint Protection:	NA (Its an upcoming Service currently date is not decided for the launch)	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	96%	
			Backup and Recovery (RPO):	NA (Part of CMDB)	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

6	Internal Business Applications	NOC infra Team			Attached Relevant Parameters in Service Report
			Availability:	24/7	
			Endpoint Protection:	Server 100%	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	NA (It applies through Authentication Services)	
			Backup and Recovery (RPO):	99.99%	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

7	Collaboration and Communication	Manager Service Desk	Availability:	Business Hours (8am to 8pm - Monday to Saturday)	Attached Relevant Parameters in Service Report
			Endpoint Protection:	NA (Maintained by supplier)	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	NA (It applies through Authentication Services)	
			Backup and Recovery (RPO):	NA (Maintained by supplier)	
			Application Management:	NA (Maintained by supplier)	

Information Technology Services Procedure

8	Security	NOC infra Team			Attached Relevant Parameters in Service Report
			Availability:	24/7	
			Endpoint Protection:	Server 100%, Workstation 90%	
			Service Desk SLA:	95%	
			Access Control Policy Compliance:	96%	
			Backup and Recovery (RPO):	99.99%	
			Application Management:	Updated versions as agreed with business	

Information Technology Services Procedure

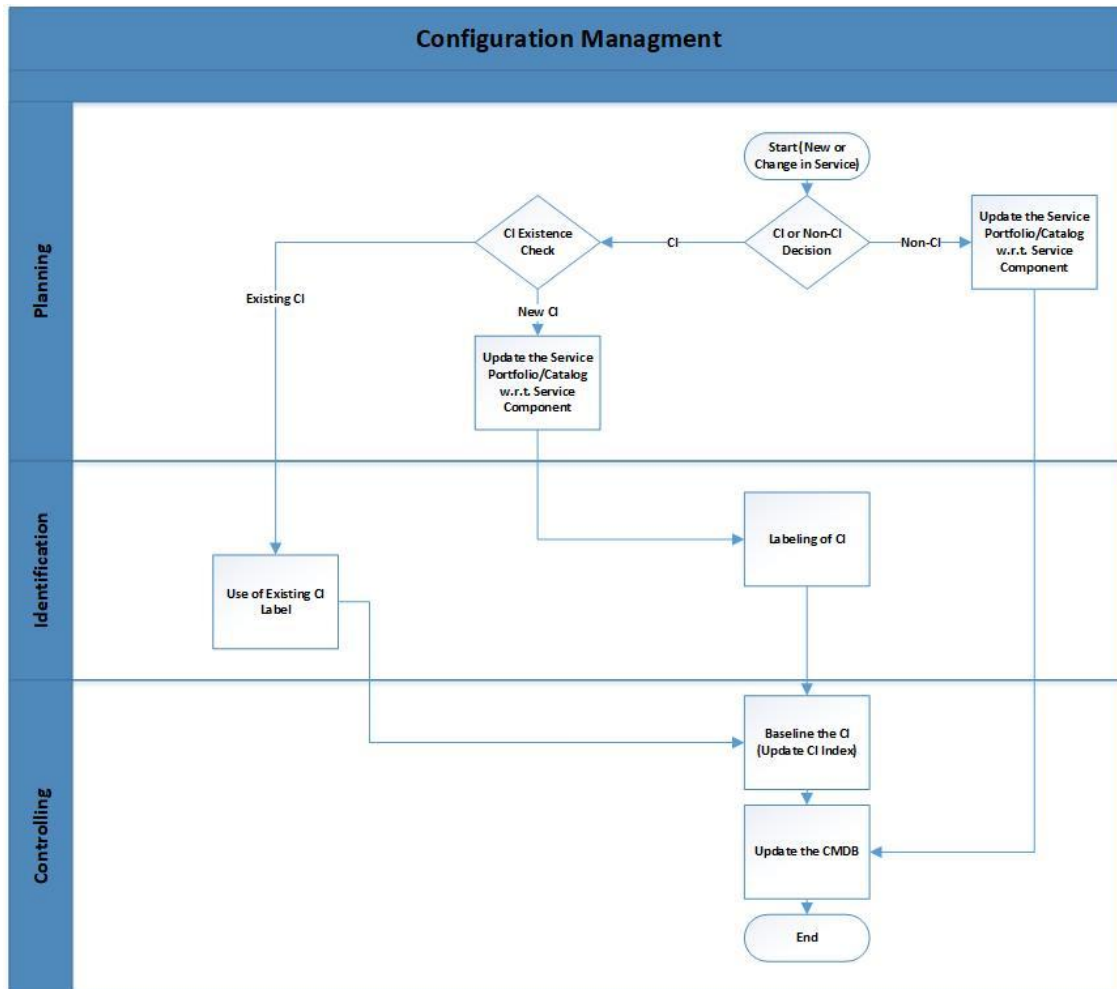
9	Data Center	NOC infra Team			Attached Relevant Parameters in Service Report
			Availability:	24/7	
			Endpoint Protection:	Server 100%	
			Data Center SLA:	99.99%	
			Access Control Policy Compliance:	100%	
			Backup and Recovery (RPO):	99.99%	
			Application Management:	Updated versions as agreed with business	

4.6 Configuration Management

Configuration Management shall be carried out by IT in consideration for three of the below categories.

- Services Configuration.
- Server, Network and VoIP Systems Configuration.
- End-User configuration.

Information Technology Services Procedure



4.6.1 Planning

Naming convention is defined for the labeling of CIs and Non-CIs Service components.

a. In Case of Non-CI

Update the Service Portfolio/Catalog w.r.t. Service Component.

Update the Service Portfolio/Catalog regarding new or change in service.

b. In Case of CI

Check for reuse the existing CI regarding new or change in service.

In case of new CI update the Service Portfolio/Catalog w.r.t. service components.

4.6.2 Identification

a. In case of New or Change in CI

In case of New CI, create the unique CI code for labeling as per CI Index.

In case of new or change in CI identify CI label if already not existing.

Information Technology Services Procedure

Identify or change the version of new CI, update existing CI version if required.

b. In case of Reuse of existing CI

In case of reuse of existing CI use existing CI label and version from CI Index.

Update existing CI version if required.

4.6.3 Controlling

a. In Case of Non-CI

Update the CMDB w.r.t. Service component described in Service Portfolio/Catalog.

b. In Case of CI

Update the CI Index w.r.t. to the case of new/change or reuse of existing CI.

Update the CMDB accordingly.

4.6.4 Services Configuration

- Manager / Assistant Manager I.T. shall be responsible to carry out selection of service provider to perform service configuration after appropriate evaluation.
- Manager / Assistant Manager I.T. shall engage required resources from Sybrid IT team to perform service configuration.
- Manager / Assistant Manager I.T. will ensure appropriate SLAs for third party services.

4.6.5 Server, Network and VoIP Systems Configuration

Systems, Network or VoIP Engineers shall be responsible to carry out the entire configuration on the following devices with the assistance of Systems, Network and VoIP Administrators.

- Application/Database Servers.
- VoIP Servers.
- Infrastructure Servers.
- Proxy Servers.
- Active Directory Servers.
- File Servers/FTP.
- Email Servers.
- Access Switches.
- IP Phones.
- Wireless Access Points.
- Network Printer/Scanner.
- Multimedia Devices.

Information Technology Services Procedure

Systems, Network or VoIP Administrator shall be responsible to carry out the entire configuration on the following devices with the assistance of Manager I.T/ Assistant Manager I.T.

- Application/Database Servers.
- VoIP Servers.
- Infrastructure Servers.
- Proxy Servers.
- Active Directory Servers.
- File Servers/FTP.
- Email Servers.
- Backup Servers.
- Access Switches.
- IP Phones.
- Wireless Access Points.
- Routers.
- Core & Distribution Switches.
- Perimeter, Edge or Data Center Firewalls.

All the configuration of above mentioned devices shall be incorporated in Configuration Management document **GIT-201 Infrastructure Configuration Management Guideline** for Karachi and **GIT-301 Infrastructure Configuration Management Guideline-ISB** for Islamabad after reviewed by Manager IT. Any change in configuration shall be performed according to **Change Management Process**.

4.6.6 End-User Configuration

Systems Support Engineer shall be responsible to carry out the entire following configuration at end user refer **GIT-204 Client End Configuration**. He will take assistance from Team Lead-

Support or System Engineer in case it is required.

- Desktop Installation/Configuration
- IP Configuration
- Software Installation/Configuration.
- Printer Configuration.
- Soft Phone Configuration.
- Email (Outlook) Configuration.
- Hardware Configuration.
- Multimedia Configuration.
- Service (Internet, VPN etc.) Configuration.

Systems Support Engineer shall be responsible to install/configure any software as defined in **RIT-217 Approved Software list**.

Information Technology Services Procedure

IT department will be responsible to update approved software list while considering operational requirement with the help of Need Analysis and considering all licensing agreement, legal & statutory requirement.

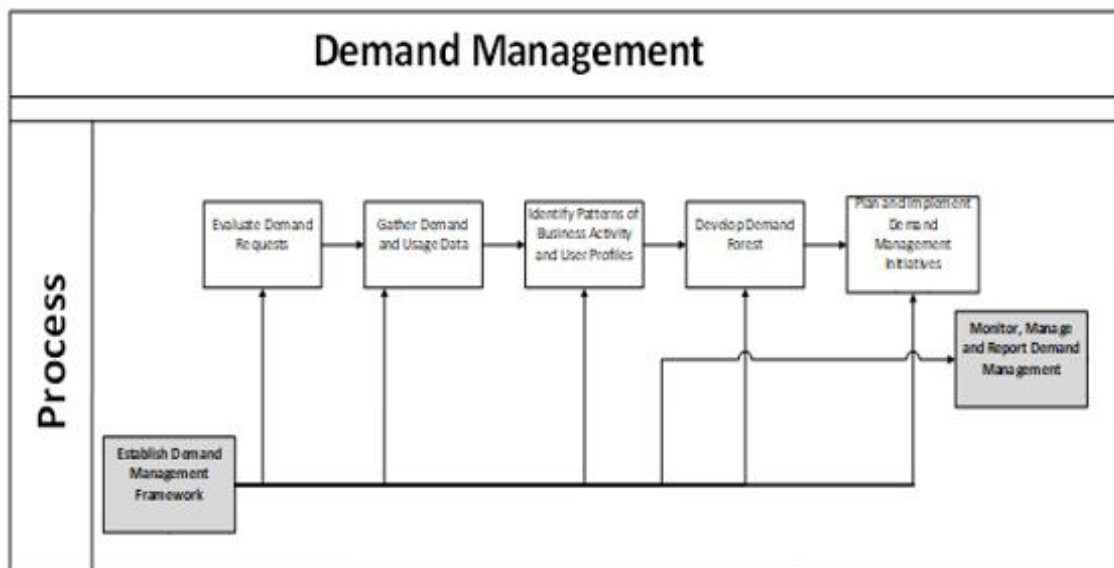
Any services or hardware access will be configured according to the access rights management process.

All the configuration of client end will be incorporated in **GIT-204 Client End Configuration for Karachi** and **GIT-304 for Islamabad**.

4.7 Procedure for Demand Management

The Demand Management process translates demand from the customer requirements in IT service terms (i.e. consumption units). It identifies gaps and misalignment between demand and service provision, proposes policies and incentives designed to minimize or close gaps. This is beneficial to planning IT capacity and other resources as required.

The process of Demand Management is applicable to the Service Owners and strategic planning personals.



4.7.1 Establish Demand Management Framework

This activity defines all direction, guidance, policies, and procedures; it also describes how to perform the process. Collectively, all of these activities are the “Demand Management process framework”. This information is reviewed in the Evaluate Process Performance activity, which generates recommendations for changes and improvements to the Demand Management process framework.

4.7.2 Evaluate Demand Requirements

This activity determines the conduit for analyzing business demand. This is important because it establishes the data collection requirements from processes that provide raw data via Knowledge Management (e.g. Request Fulfillment and Capacity Management). The execution of this activity is advised to properly establish strategy prior to the collection, analysis, and subsequent decisions that occur in Demand Management.

Information Technology Services Procedure

4.7.3 Gather Demand and Usage Data

This activity collects and consolidates demand data from multiple sources for further analysis. A comprehensive analysis of demand is used for demand forecasting and initiative evaluation based on capacity measurement sheet.

4.7.4 Identify Patterns of Business Activity and User Profiles

In this activity, patterns of end-user behaviors are evaluated and used to synchronize consumption (demand) with capacity (supply) of IT Resources. Incoming data and known upcoming initiatives from Service Portfolio Management are helpful to determine requirements for the Demand Management process.

4.7.5 Develop Demand Forecast

This activity uses the service demand baseline and collected data along with aggregated historical data to generate a demand forecast. This forecast shall provide insight to upcoming demand requirements, including expected high/low demand periods.

4.7.6 Plan and Implement Demand Management Initiatives

This activity uses Demand Forecast information to predict misalignment between demand and supply of IT resources and services. It creates strategy to realign resources and services through policy, incentives and/or IT resource investment. When a decision to shape demand through incentives is made, analysis is performed to shape demand through methods such as Incentives and Penalties. This activity concludes with the formulation and communication of a prioritized set of recommendations (e.g. Plans of action, investment recommendations, etc.)

4.7.7 Monitor, Manage and Report Demand Management

In this activity, all Demand Management process is monitored to determine whether suitable progress is made. In case of unsatisfactory results, the resultant actions can be suggested to ITSM steering team via email.

Information Technology Services Procedure

4.8 Change Management

4.8.1 Change Management Obligation

Change management will be implied according to the change management guidelines **GISM- 901** involves following access types which are controlled by Sybrid IT. Change Management requests will be initiated by concern if there is any change is required for the following categories:-

- Configuration Changes in Internal/External Services.
- Network/ Infrastructure Architecture (Servers, Switches Routers, firewall.)
- Movement of Fixed Asset.

Sybrid classified changes in 03 major types as mentioned below:

- **Standard changes** are changes at end user or any policy or procedure due to business requirements. Since these changes are also subject to established policies and procedures, they are the easiest to prioritize and implement, and often don't require approval from a risk management perspective.
- **Normal changes** are those that must go through the change process before being approved and implemented. If they are determined to be high-risk, a HoD/Manager/AM must approve whether they will be implemented. Changes in configuration and architecture due to upgrade or implementation of new technology will be considered in normal changes.
- **Emergency changes** arise when an unexpected error or threat occurs, such as when a flaw in the infrastructure related to services needs to be addressed immediately. A security threat is another example of an emergency situation that requires changes to be made immediately. Changes in configuration and architecture in case of any technology failure or disaster to restore services will be considered as emergency changes.

4.8.2 Change Management Request for Services and Network/Infrastructure

- Any Change for configuration of services, Network or Infrastructure must be reviewed by Manager/A.M. IT for any vulnerability, potential and information security risk and possible service impact associated with the requested change.
- Manager/A.M. IT shall approve or disapprove the changes after technical evaluation with proper justification and reasoning.
- Manager/A.M. IT must ensure fallback procedure (considering the particular situation) in case of any disaster/failure that can occur after performing configuration.
- All the changes requested will be logged and maintained on **RIT-201 Change Management Form**.

Information Technology Services Procedure

4.8.3 Change Management Request for Movement of Fixed Assets

- Any Change Management request shall be generated by Sybrid employee via Change management form CMF
- User must define the following information while generating this request.
 - Change Type:
 - Resource Name:
 - Reason:
 - Change Required:
 - Source:
 - Destination:
- Any request must be reviewed and approved by respective reporting authority prior to access granting.
- Any request must be reviewed and approved by Sybrid IT prior to performing change.
- Sybrid IT and C&A has right to disapprove any request considering the need analysis, risks and chances of data theft or information leakage.
- After incorporate change Sybrid IT Team will update Asset Inventory on Portal.

4.8.4 Change Management Review

- Any Change will be reviewed on a monthly basis sequentially on data share as mentioned in the change management report/form for a specific area in a cycle to ensure review of all changes.
- After the review completion, change management report will be forwarded to ISM for verification.

4.9 Asset Management

4.9.1 I.T. Acquisition / Requisition Process

- ? Departments identify the need for acquisition/requisition of a product through the relevant manager using **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202 IT Requisition form** for Islamabad.
- ? Users will also initiate request on I.T. Ticketing System.
- ? The relevant line manager is responsible for assessing the need for the required product and forwarding it to the IT Manager.
- ? IT Manager will perform need assessment and approve/disapprove on need basis.
- ? Sybrid IT will check if any existing inventory can be accommodated to fulfill the need in this case.
- ? IT Team with IT Managers approval is responsible for technical assessment of the purchase requisition.
- ? IT Team with IT Managers approval forward the requisition with complete specification details to Admin department.
- ? IT Team forwards the requisition with quotation and CEF or Expenditure form to the initiator of the requisition for budget confirmation/approval as per finance approval matrix.
- ? After receiving approved CEF or Expenditure, Sybrid IT submits the requisition to

Information Technology Services Procedure

Admin Department.

- ❑ Administration verifies the approval and initiates PO for vendor.
- ❑ Products are received and checked by IT Team according to **RAD 403 for KHI or RIT-202** for ISB.
- ❑ Finance will paste a tag on the product and System Support Engineer will update inventory on asset inventory sheet.
- ❑ Initiator receives the resolution email from system, and confirms the completion of the request, and close the ticket on Complaint Management System If user is not satisfied then the ticket will be re-assigned to IT Support Executive.

4.9.2 Equipment Issuance

- ❑ Departments identify the need for replacement of a product through the relevant supervisor using **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202**.
- ❑ The relevant line Manager is responsible for assessing the need for the required product.
- ❑ Request will be forwarded to Manager/AM IT by sending **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202 IT Requisition form** for Islamabad.
- ❑ IT Team will issue the inventory according to the request in **RAD-403 Stock issuance & purchase requisition** for Karachi & **RIT-202 IT Requisition form** for Islamabad.
- ❑ IT Team will deliver the required products as per the request of end user.

4.9.3 I.T. Inventory Management

- ❑ Sybrid IT Team will maintain asset inventory on ERP portal.
- ❑ Sybrid IT will maintain its backup inventory on **RIT-205 Backup Inventory** for all the desktops, laptops, head gears and LCDs.
- ❑ Sybrid IT will maintain Data Center equipment inventory on **RIT-205 Backup Inventory** for all servers, switches, routers and other equipment's.
- ❑ Sybrid IT Asset inventory will be reviewed by Manager/A.M. I.T.

4.9.4 Secure Disposal and Reuse of I.T Equipment

It includes the process; regarding steps to be taken by I.T support executives for reuse and disposal of I.T equipment.

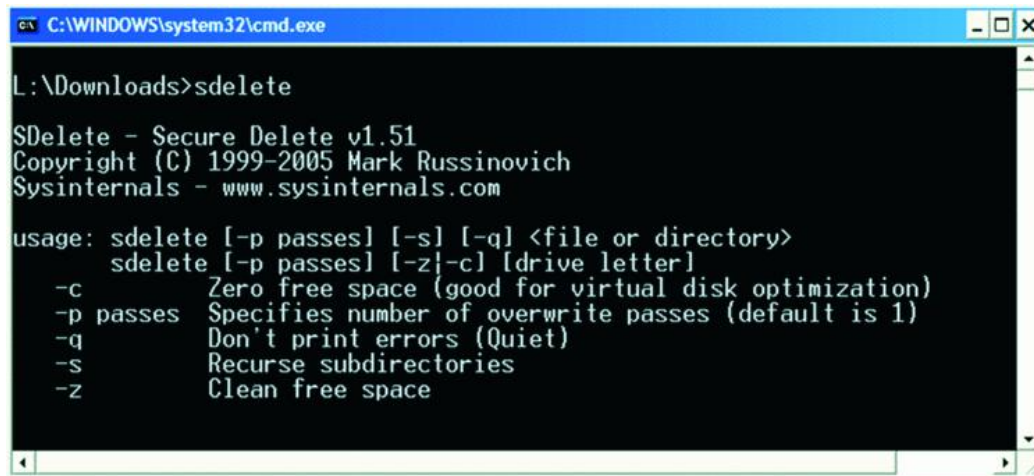
I. Reuse:

For reuse of storage media, I.T support executives will use "SDELETE" (File Shredder Software) utility to clean the media. Before assigning it to any employee, Steps for using SDELETE are mentioned below:

- sdelete [-p passes] [-s] [-q] <file or directory> , sdelete [-p passes] [-z|-c] [drive letter]
- -c (Zero free space (good for virtual disk optimization)).

Information Technology Services Procedure

- -p passes (Specifies the number of overwrite passes (default is 1))
- -q (Don't print errors)
- -s (Recurse subdirectories [Note: The contents of all subdirectories are included in the deletion or disk wipe.])
- -z (Cleans free space [Note: this is similar to the -c option except -z uses a random string of values to more securely wipe free disk space.])



```

C:\WINDOWS\system32\cmd.exe

L:\Downloads>sdelete

SDelete - Secure Delete v1.51
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: sdelete [-p passes] [-s] [-q] <file or directory>
       sdelete [-p passes] [-z|-c] [drive letter]
-c      Zero free space (good for virtual disk optimization)
-p passes Specifies number of overwrite passes (default is 1)
-q      Don't print errors (Quiet)
-s      Recurse subdirectories
-z      Clean free space
    
```

II. Secure Disposal:

If I.T support executive found any equipment to be dead or no possibility of its reuse is found then secure disposal of equipment will be necessary. Below are the steps for secure disposal:

- I.T support executive will check for any possibility; if equipment can be reused.
- If the equipment is reusable then above mentioned process of Reuse will be followed.
- If I.T support executive found equipment to be dead then it will be provided to Administration Department.
- Upon receiving the equipment from I.T, admin will break the storage into pieces so that it can be shred securely.
- I.T will then modify its asset inventory accordingly and update these equipment details in **RIT-231 Disposal List**.

4.10 Access Rights Management

Access rights management will be performed according to **ISMP-902 Access control policy**. Regarding the I.T.'s domain it involves following access types controlled by Sybrid IT.

- Internet Access
- Internal Network Access
- Printer/Scanner

Information Technology Services Procedure

- File Server/FTP Access
- Any request must be reviewed and approved by respective reporting authority prior to access granting.
- Access can be of two type "Temporary" or "Permanent", temporary access will be revoked on completion of provided date and permanent access will be revoked on termination of services of an employee.
- Any request must be reviewed and approved by Sybrid IT prior to access granting while considering need analysis, all kinds of risks and ripple effects.
- Sybrid IT and C&A has right to disapprove any request considering the need analysis, risks and chances of data theft or security leakage.
- User must define the following information while generating this request.
 - Access Type: Read, Read & Write, Application or Website
 - Resource Name: (Name of resource on which access is required)
 - Justification: (Business requirement for this access type)
 - Required access from: (Date from which access is required)
 - Required access till: (Date till which access is required)

4.10.1 Internet/ Wireless Access

- Any Internet resource (Website, Wireless, VPN etc.) access request shall be generated by Sybrid employee via Sybrid Workflow erp.sybrid.com/Workflow/Access Rights on ERP Portal for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.
- After all approvals support engineer saves the WIFI password and assign an IP to the device himself from centralized IP sheet and then update the IP sheet accordingly.
- System Engineer will grant any approved access to the internet from proxy servers.
- In case there is a change in any access policy defined at proxy server it will be done according to change management.

4.10.2 Internal Network

Any Internal Network resource access request shall be generated by Sybrid employee via Sybrid Workflow on ERP Portal erp.sybrid.com/Workflow/Access Rights for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.

4.10.3 Printer/Scanner

Any Data resource access request shall be generated by Sybrid employee via Sybrid Workflow on ERP Portal for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.

- Support engineer will provide printer/scanner access after

Information Technology Services Procedure

all approvals as defined in **GIT-204 Client End Configuration**

4.10.4 File Server Access

Any File Server resource access request shall be generated by Sybrid employee via Sybrid Workflow on ERP Portal for Karachi where as he/she will fill **RIT-214 Access Rights Form** for Islamabad.

- System Engineer will provide any access after all approvals on Data/Folder which shall be followed according to **GIT-202 Data Management Guideline** for Karachi and **GIT-302 Data Management Guideline-ISB**

4.11 Access Rights Review

- Access Rights will be reviewed on a monthly basis sequentially on data share as mentioned in the review access right report for a specific area in a cycle to ensure review of all access rights by using this link [http://erp.sybrid.com/Access right review report](http://erp.sybrid.com/Access%20right%20review%20report) only for Karachi site.
- Manager/AM IT will review all the rights of internal network, servers, administrator access of servers using server audit software (for Microsoft servers) whereas for linux servers it will be reviewed from its default user lists.
- Manager/AM IT will review all the rights of Internet access from proxy servers.
- QA have the rights to review all the access requests which were being granted to users.
- For Islamabad Site all the access rights will be reviewed with the record document **RIT-215 Review Access rights Form**.

4.12 Information Security Management

- All the configuration details of every parameter regarding below mentioned procedures will be applied according to **GIT-201 Infrastructure Configuration Management Guideline & GIT-301 Infrastructure Configuration Management Guideline-ISB** for Karachi and Islamabad respectively.
- Any unauthorized person does not have access to these resources; any login attempt shall be denied.
- Sybrid IT must ensure that no user has rights to install any software, utilities, patches, drivers or any kind of application unless there is a severe business need which is justified and meeting the information security requirements.
- The privileged access rights are prohibited in Sybrid, but the allocations of these rights are given after formal approval from the top management via email and using the same process.
- Sybrid IT must ensure that no user has rights to install any software, utilities, patches, drivers or any kind of application unless there is a severe

Information Technology Services Procedure

business need which is justified and meeting the information security requirements.

- All the privilege access users will be listed in **RIT-230 Privilege access user list** along with the details of their privileged access and authorities. These details will be shared with ISM on quarterly basis.
- Any privileged user access rights will be reviewed by Manager IT /A.M. IT on quarterly basis and Manager IT/AM IT rights will be reviewed by ISM.

4.12.1 Event Logging

Types of logs being reviewed;

- Active directory log.
- Proxy server logs.
- Microsoft Exchange Server Logs.
- VoIP Server Logs.

Authorized personnel who have rights to view and export logs;

- Manager/A.M. I.T.
- Systems Engineer/Administrator

People authorized to log extraction and review request;

- IS Manager
- Manager/ A.M. I.T.

System Engineer/Administrator logs will be reviewed by Manager/AM IT & Manager/AM IT logs shall be reviewed by ISM on monthly basis.

These Logs for Microsoft Servers will be reviewed by server audit software whereas for linux servers it will be reviewed by its default feature.

4.12.2 Network Security & Management

In order to networks with segregated environment for end-users, servers and devices we have got:

- i. Separate VLANs implemented for:
 - a. Network device management.
 - b. End-user traffic separation from the server network.
 - c. Server traffic separation from the end-user network.
- ii. Server network protection from direct access from the internet via a PERIMETER Network firewall.
- iii. Wireless network implementation of WPA2-PSK.
- iv. Sybrid IT must ensure that no user has access to change any Network Privileges.

4.12 Email Transmission

Employee will have a limited access of sending and receiving of emails, employee can only send/receive emails at sybrid.com/sybridmd.com/sybridts.com

Information Technology Services Procedure

exchange domains. Email access will be extended with due justification of business needs considering the security impacts.

a. Encrypted Emails

All emails that contain either Text / Attachments would be sending via controlled Google Email Services and Microsoft Exchange Server with encrypted emails.

b. Authorized access

Sybrid IT will provide authorized restricted access of emails for each employee at the request of employee's line manager mentioning in new starter form.

c. Access Levels

Sybrid IT will provide following mentioned email access on the basis of request these accesses includes

- Local Email Access
- External Emails Access (Inbound/Outbound)

4.12.4 User Account Management

SYBRID associates will require a unique id to access SYBRID domain Server, network, corporate applications, SharePoint portal, Servers and applications. This ID will be created on our AD server at the time employee joins organization. User account management will be the responsibility of systems engineer.

- Every associate in SYBRID have a unique login identity.
- For a new hire id request will be generated by HR through **RIT-102 Employee Starter Form**.
- This form will have the information of new employee and the access he or she required.
- In case of any movement from one campaign to another or from one department to other HR will inform us, so the access will be modified accordingly.
- HR will share the list of existing employees department wise with IT on quarterly basis which can be match up with the list of user account on the AD server and email server.
- In case of any discrepancy a security incident will raise to Information security manager.
- If any employee resigns, HR will proactively intimate IT by initiating separation notification and **RIT-101 Employee Transfer/Leaver Form** so his/her access rights will be revoked.
- Due to unique customer requirements, in case of employee resignation/transfer for business unit **Sybrid TS** business managers will share **RIT-204 TS Employee Leaver Transfer** form for separation process.

4.12.5 Anti-Malicious

a. Anti-Virus Setup

- Centralized Antivirus Server is deployed in our network to secure information facility from malicious viruses and Trojans.

Information Technology Services Procedure

- There is a client / server based solution so clients are not directly received their updates from internet and only internal server is responsible to receive all updates from Internet.
- Server is directly connected with the internet and downloads all necessary updates regularly.
- All Client PC's are fully scanned on weekly basis.
- Network sharing is also limited through antivirus server to ensure clean network.
- USB Mass storage Access is restricted with the help of Centralized Antivirus.

4.12.6 Drive Encryption

All laptops that carries company confidential information will have their drives Encrypted by using any Encryption scheme algorithm based software / Technique to maximize the security of data if incase of theft of employee's laptop.

a. Encryption Activity

- Using 3rd party Software or Microsoft windows features, System Support Engineer ensures the full drive encryption before handing over the laptop to the employee.
- System Support Engineers will make sure that all mobile devices storage media are encrypted with defined mechanism at the time of initial/re-configuration of device prior to handing it over to users.
- All encryption keys will be saved in a file and it will be placed at a centralized location accessible to all IT Team members.

b. Decryption Activity

- System Support Engineer must make sure the drive Decryption before performing OS Reinstallation, Drive Formatting & Drive Partitioning on employee's laptop to ensure data integrity & unwanted data loss.

4.12.7 Secure Communication and Infrastructure

There will be always secure communication channel would be provided if in case Sybrid needs to communicate with remote site or server that contains confidential data including EPHI.

a. Secure Infrastructure / LAN

All the internal servers and client machines would be at the back of a firewall that will ensure and maximize the protection and guard against the brute force attacks and vulnerabilities.

Information Technology Services Procedure

- b. Secure Communication with Remote Sites & Customer Network
- All the communication with remote Sites and customer network will be carried out with any of below mentioned two methods:
- Secure Site to Site IPsec VPN.
 - Point to Point L3 MPLS connectivity.

4.12.8 Patch & Technical Vulnerability Management

Patch & Technical Vulnerability Management for all the Microsoft Operating Systems (Client/Server) shall be conducted by a centralized patch management system of Microsoft System Center Configuration Manager/ WSUS.

Only selected and important updates related to windows OS and software (Office, SharePoint etc.) are being reviewed and pushed by IT department and all systems are updated via windows automatic update.

If there is vulnerability identified/observed but there is no suitable countermeasure. In this situation, the Sybrid IT team should refer to forums and concerns subject matter experts depending on criticality of risks associated to such vulnerability and suggest appropriate corrective actions as suggested by such forums or subject matter experts and practice across the industry.

4.12.9 Resource Usage Logs

a. Internet Usage Log

Internet usage log will be maintained on Internet security Server and reviewed monthly by System Administrator using proxy server's reports.

b. Access Control Log (like invalid login attempts on logon)

Access Control Logs will be monitored through system audit and policies by System Administrator by using server AD audit software.

c. Administrator Logs review

Manager IT/ AM IT shall review the logs of administrator privileged IDs on the following devices.

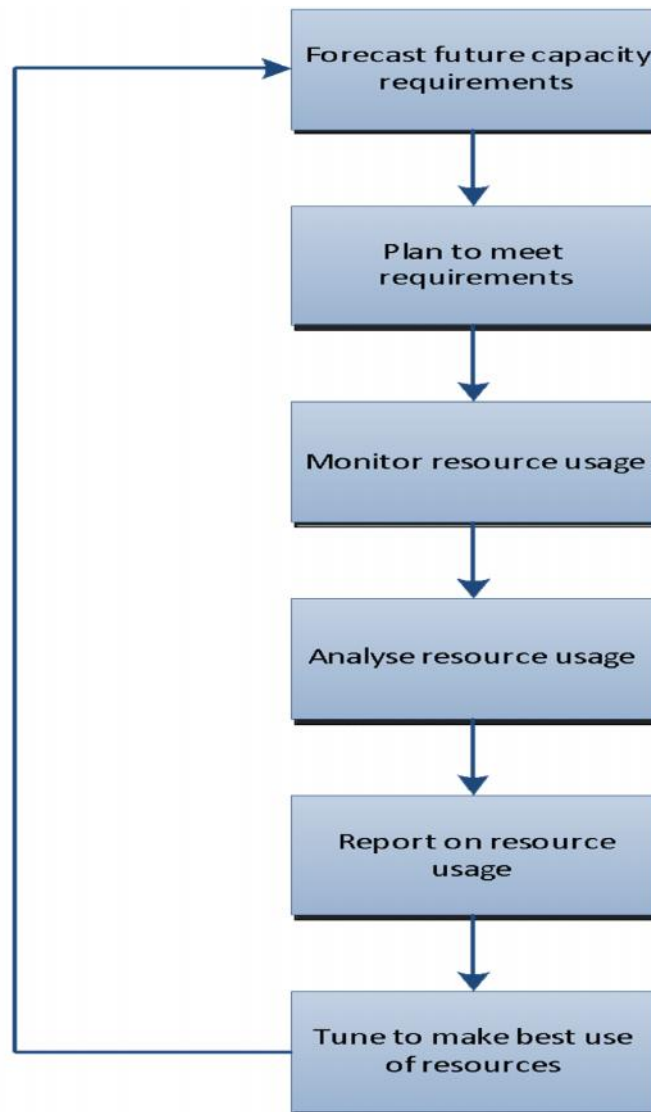
- Active Directory Servers by using AD audit software
- FTP/ File Servers by using AD audit software
- VoIP Servers by Linux default feature
- Application Servers by using AD audit software

4.13 Capacity Management

The use of resources should be monitored, tuned, and projections made for the future capacity requirements to ensure the required system performance.

Information Technology Services Procedure

The process of capacity management is shown in the following diagram:



4.13.1 Forecast Future Capacity Requirements

The purpose of this step is to capture and understand the changing business requirement for capacity. This may take a number of forms, such as:

- increasing or decreasing use of existing applications by current users
- the addition or removal of users
- a change in the way the system is being used e.g. the introduction of a new batch job that must be run during the working day

Information Technology Services Procedure

- a change in the days and/or times the services are used e.g. beginning Saturday working or overtime

Such changes may have an effect on a number of areas of infrastructure such as server processor and disk capacity or network bandwidth as well as upon other resources such as people and facilities engaged in delivering the service.

In order to gain as much advance knowledge of such changes as possible, business capacity requirements will be a key area addressed at each service review meeting and will be a standard agenda item. These meetings will be documented and items affecting capacity management will be fed into the overall capacity plan.

4.13.2 Plan to Meet Requirements (Capacity Planning)

For each identified service provided by Internal ITS Department and defined in the service portfolio/ Service Catalog, an estimate of future capacity adjustments will be made.

A capacity plan will be produced on an annual basis which will bring together the future demands on service components from business changes and the current utilisation of resources and identify any areas in which the provision of capacity needs to be adjusted. This may involve the justification of additional hardware such as server upgrades or the recruitment of additional support staff, amongst other proposals.

Key to this task will be the understanding of which service components underpin each service and the dependencies between them. For shared resources such as file and print servers and domain controllers for example, the net impact of changes across all business areas must be considered.

Although initially produced on an annual basis, the capacity plan will be subject to amendments as and when significant changes are made to business requirements or to the infrastructure. These amendments will be made under the control of the change management process.

a. Method Used

Information concerning future usage of key services is collected as part of the regular service review process, and is a standard item on the agenda of each meeting. Customers are asked to highlight any known increases or decreases in the usage of existing services and any other business events likely to impact on the effective provision of service.

Data regarding the current usage of technical resources is collected via a number of monitoring tools (such as SolarWinds/Windows Performance Monitor etc.) and is analysed quarterly to identify trends.

b. Assumptions Made

In preparing this plan, the following assumptions have been made:

- Forecasts of future use are accurate, both in terms of timing and degree of change
- Measurements of current capacity usage are representative of typical Service Level Requirements (SLRs)

These assumptions will be reviewed on a semi-annual or on need basis to assess their continued validity.

4.13.3 Current and Forecast Demand for Services

There are a number of key business, technical, statutory, regulatory and contractual aspects that could potentially have an impact upon the capacity of the service in the timeframe under

Information Technology Services Procedure

consideration. It depends on the following:

- Maintain the current
- Changes Affecting Capacity Requirements
- Trends
- Impact of Agreed Availability, Service Continuity and Service Level Requirements.

All above considerations shall be addressed through procedure for Demand Management and output shall be documented in capacity measurement sheet.

4.13.4 Service and Resource Summary and Recommendations

By using following reference document, we can summarize the current capacity usage of the key components of the IT services, changes forecast over the current financial year, and recommendations for change made to ensure that sufficient capacity is provided to cope with the changes expected.

Ref: Business Forecasting and Capacity Planning KHI Site

a. Impact of New Technologies and New Techniques

ITS Department continuously require a careful assessment of the capacity implications to analyse the impact of new technologies and new techniques before adding to the environment.

b. Predictive Analysis

Predictive analysis to be carried out beyond a basic level. This area will be looked at in the longer term. In the meantime this will take the form of extrapolation of identifiable trends to pinpoint when thresholds on resources such as disk space will be reached.

4.13.5 Monitor, Analyze and Report on Resource Usage

In order to understand the current use of our resources, where possible software tools will be used to record the utilization of key components. As a minimum, these will be:

- Server processor capacity
- Server Memory capacity
- Server disk capacity
- Network port capacity
- Network bandwidth capacity
- Client Name
- Floor
- Business Unit
- Services
- Location
- Existing State
- Forecast Uplift
- After Uplift Projection

Where feasible, this data will be collected continuously and stored for historical reporting purposes. A threshold will be set for key resources (such as disk capacity) so that an alert is generated if that threshold is exceeded, allowing immediate action to be taken.

Information Technology Services Procedure

4.13.6 Tune to Make Best Use of Resources

In addition to monitoring the actual usage of key resources, regular attention will also be paid to the correct setup and tuning of servers and network devices so that best performance can be obtained from the available resources.

This will cover issues such as:

- Memory allocation
- Swap space sizes
- Job priorities
- Identification of resource bottlenecks

An annual exercise will be carried out on all business-critical servers. All changes identified will be implemented under strict change management control.

4.13.7 Component Capacity Management

Alerts are configured on individual servers and a threshold is defined for hard drive, CPU and Memory utilization when the utilization exceeds the threshold it generates alert in event logs.

- System Engineer is responsible to perform regular maintenance activity to identify bottle necks and other issues.
- Utilization of resources is monitored on regular basis in maintenance activity such as hard drive, CPU and Memory utilization.
- Event logs are also regularly monitored in maintenance and logged in maintenance reports.
- Any issues will be escalated to Manager/AM IT for further actions.

4.13.8 Service Capacity Management

Service Capacity management will be regular practice and IT will update the stake holders quarterly for Telephony, Internet, Email and other services through Service Capacity Report.

- IT will review the services according to the service capacity report on quarterly basis
- IT Manager will share the Service capacity report with all the stake holders.
- Stake holders will provide the approval on action items
- IT will proceed on action items and shared the updated service capacity report

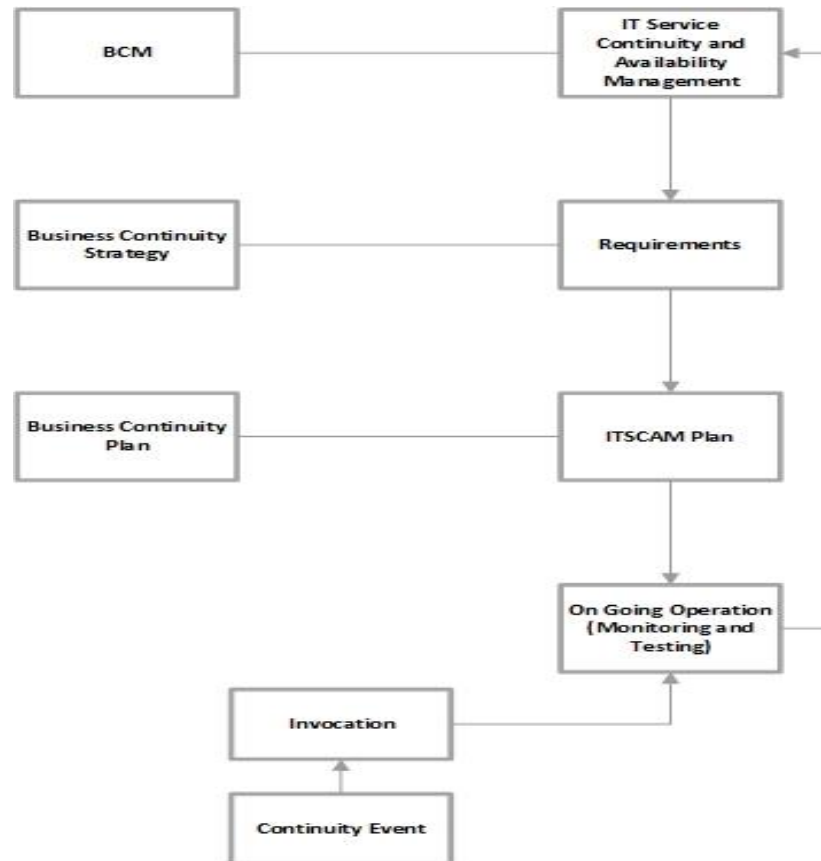
4.13.9 Business Capacity Management

Business capacity management service capacity report will be shared with the BD Team and BD will share the new business forecast analysis so IT can ensure that future business requirements are translated into quantifiable IT services.

- IT will share the service capacity report with BD Team on quarterly or requirement basis.
- BD Team will share the new business forecast analysis on quarterly basis

Information Technology Services Procedure

- IT will share the action items according to the forecast analysis.
- Stake holders will provide the approval on action items
- IT will proceed on action items and shared the updated service capacity report.



4.15.1 Service continuity and availability requirements

- Ascertaining the business requirements for IT service continuity and availability are critical component in order to determine how well ITS department will survive a service interruption or disaster. If the requirements analysis is incorrect, or key information has been missed, this could have serious consequences on the effectiveness of IT Services continuity and availability.
- ITSM steering team shall perform services impact analysis in accordance with Risk Management Procedure in order to reduce the risks of service interruption or disaster and suggest recovery options as the treatment of the risk scenario.
- The results of the Service Impact Analysis and the Risk assessment will enable appropriate IT Service Continuity and availability strategies to be produced in line with the service needs. The strategy will be an optimum balance of risk reduction and recovery or continuity options. This includes consideration of the relative service recovery priorities and the changes in relative service priority for the time of day, day of the week, and monthly and annual variations. Those services that have

Information Technology Services Procedure

been identified as high impacts in the short term within the services risk management will need to concentrate efforts on preventative risk reduction methods – for example, through full resilience and fault tolerance – while an organization that has low short-term impacts would be better suited to comprehensive recovery options.

4.15.2 Service continuity and availability plan

- Once ITSM steering team conducted Service Impact Analysis, the IT Service Continuity and Availability Plan shall be produced in line with the Service Risk Assessment.
- IT service continuity and availability plan shall be developed to enable the necessary information for critical systems, services and facilities to either continue to be provided or to be reinstated within an acceptable period to the business.
- Generally, the Service Continuity Plan rely on the availability of IT services, facilities and resources. As a consequence of this, IT service continuity and availability plan need to address all activities to ensure that the required services, facilities and resources are delivered in an acceptable operational state and are 'fit for purpose' when accepted by the business. This entails not only the restoration of services and facilities, but also the understanding of dependencies between them, the testing required prior to delivery (performance, functional, operational and acceptance testing) and the validation of data integrity and consistency.
- Each critical service owners are responsible for the development of a plan detailing the individuals who will be in the recovery teams and the tasks to be undertaken on invocation of recovery arrangements.
- The IT service continuity and availability plan must contain all the information needed to recover the IT systems, networks and telecommunications in a disaster situation once a decision to invoke has been made, and then to manage the business return to normal operation once the service disruption has been resolved. One of the most important inputs into the plan development is the results of the Service Impact Analysis conducted by ITSM steering team. Additionally other areas will need to be analysed, such as Service Level Agreements (SLA), security requirements, procedures and external contracts.

4.15.3 Service continuity and availability monitoring and testing

- ITSM Steering team is responsible for the periodic or ad hoc monitoring and review of the IT Service Continuity and Availability management, also ensures that strategies are up to date, and incorporates lessons from testing.
- Governance, Strategy and Planning will coordinate annual reviews, and prepare a testing schedule for all Service Continuity Plans.
- This monitoring, review and testing is part of ongoing operations and for this ITSM steering team needs to ensure that all staff are of the implications of IT Service Continuity and Availability and these as part of their normal working, and that everyone involved in the Service Continuity Plan has been trained in how to implement their assigned actions.
- Invocation is the ultimate test of the Service Continuity and IT Service Continuity and Availability plan. If all the preparatory work has been successfully completed, and plan developed and tested, then an invocation of the IT Service Continuity and Availability plan should be a straightforward process, but if the plans have not been

Information Technology Services Procedure

tested, failures can be expected.

- The invocation and initial recovery is likely to be a time of high activity, involving long hours for many individuals. This must be recognized and managed by the recovery team leaders to ensure that breaks are provided and prevent 'burn-out'. Planning for shifts and handovers must be undertaken to ensure that the best use is made of the facilities available.
- Once the recovery has been completed, the business should be able to operate from the recovery site at the level determined and agreed in the strategy and relevant SLA.

4 Associated Policies/Processes/Guidelines:

S. No.	Reference Number	Records Title
1	GIT-201	Infrastructure Configuration Management Guideline
2	GIT-202	Data Management Guideline
3	GIT-203	Data Backup and Restoration Guideline
4	GIT-204	Client End Configuration Guideline
5	GIT-301	Infrastructure Configuration Management Guideline- ISB

Information Technology Services Procedure

6	GIT-302	Data Management Guideline-ISB
7	GIT-303	Data Backup and Restoration Guideline-ISB
8	GIT-304	Client End Configuration Guideline-ISB
9	ITS-REC-007	ITSM steering team structure
10	ITS-POL-001	Information Security Policies
11	ITS-POL-002	ITS Policies

5 Associated Records:

Sr. #	Reference Number	Document Title
1	RIT-101	Employee Transfer/Leaver Form
2	RIT-102	Employee Starter Form
3	RIT-201	Change Management Form
4	RIT-202	IT Requisition Form
5	RIT-203	Service Incident Report
6	RIT-204	Sybrid TS Employee Leaver/Transfer
7	RIT-205	Backup Inventory
8	RIT-209	IT Uptime Report
9	RIT-210	Customer Requirement Form
10	RIT-211	Maintenance Report
11	RIT-212	System Health Check Report
12	RIT-213	System Audit Report
13	RIT-214	Access Rights Form
14	RIT-215	Review Access Rights Form
15	RIT-216	Testing Results
16	RIT-217	Approved Software List
17	RIT-218	Onsite Backup Log
18	RIT-219	Offsite Backup Log
19	RIT-221	Daily UAN Audit Sheet
20	RIT-222	Daily Network Monitoring Sheet
21	RIT-223	Daily Server Monitoring Sheet
22	RIT-224	IT Resource Training Record
23	RIT-225	Daily IT Floor Checklist-Sybrid MD
24	RIT-226	Daily IT Floor Checklist-Sybrid CS
25	RIT-227	IT Project Action Plan
26	RIT-228	IT Business Case
27	RIT-229	Daily IT Floor Checklist-Sybrid TS
28	RIT-230	Privilege Access user List

Information Technology Services Procedure

29	RIT-231	Disposal List
30	RAD-403	Stock issuance & purchase requisition
31	ITS-REC-001	CI Index
32	ITS-REC-002	CMDB
33	ITS-REC-003	Service management plan
34	ITS-REC-004	Service performance log
35	ITS-REC-005	Service portfolio
36	ITS-REC-006	Service risk register