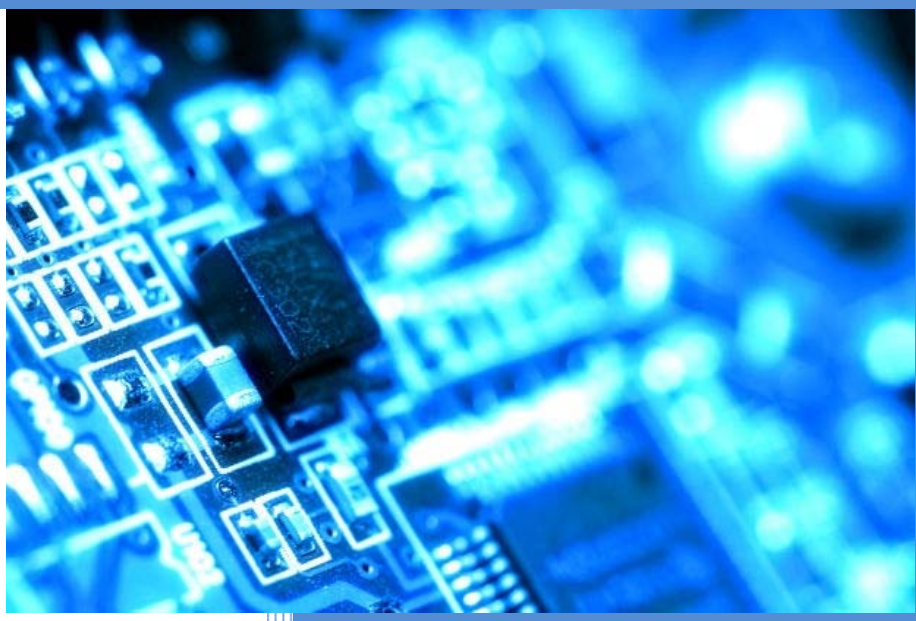
IDAHO
CONSOLIDATED SERVICES

2010

ICS Operations & Policies Manual



For State Agencies Providing and Using Consolidated Services

This manual is intended to be an Idaho state operations process framework based on the Information Technology Infrastructure Library (ITIL). It is for use by all IT Service Management (ITSM) customers, users, Support Center Managers, and Level 1 and 2 Service Technicians at agencies using state consolidated services.

Purpose and Use of this Manual

- To ensure that agency and central support Office of the Chief Information Officer (OCIO) personnel have the same understanding as to how **incidents, changes, problems,** and **releases** are handled, how **IT assets** are tracked, and what **services** are offered.
- To provide a reference document for implementing or following ITIL business process flows.
- To facilitate training for all new Help or Service Desk personnel.
- To reinforce the common language critical to understanding and applying ITIL. Because everyday words acquire specific meanings in this context, readers are encouraged to use the appendices liberally.

Organization

This manual is organized into eight chapters as follows:

Service Support	1. **Incident Management covers the process for managing the lifecycle of unplanned interruptions or reductions in the quality of an IT service.** 2. **Change Management covers the process for controlling the lifecycle of changes made to a configuration item (CI).** 3. **Problem Management covers the process for investigating the cause of incidents.** 4. **Release Management covers the planning, scheduling and controlling of the movement of releases to test and live environments.** 5. **Configuration Management helps record and track IT resources throughout their lifecycles.** 6. **Asset Management tracks IT assets and their costs throughout their lifecycle within an organization.**
Service Delivery	7. **Capacity Management helps organizations make sure their IT resources can meet their business demands, ensuring service delivery.**
Service Design	8. **Service Catalog provides a list of services offered by OCIO, their characteristics, objectives, costs, and how to access the services.**

Additionally:

- the content of each chapter is sequenced according to its lifecycle, and
- types of calls, a list of ITIL acronyms and terminology, sample graphs and accompanying resource documents are found in Appendices.

Update Process

Changes will be issued by the Enterprise Services Oversight Committee. If a user of this manual identifies a suggestion for improvement or omission, they should notify this committee. The master version of this manual will be maintained on the OCIO web site.

Table of Contents

Chapter 1: Incident Management 1.1
Overview 1.1
High-level Incident Management Narrative 1.1
Incident Management Process Flow 1.2
Roles and Responsibilities 1.3
Support Levels Defined 1.3
Incident Identification 1.3
Incident Logging and Preparation for Escalation to Level 2 ..... 1.3
Categorization 1.4
Setting Priorities 1.5
Major Incident Process 1.6
Management Escalation Process 1.6
Management Escalation Criteria 1.7
Management Escalation Process 1.7
Incident Closure 1.7
Incident re-opening 1.7
Metrics 1.7
Training for ICS Incident Management Operations 1.9
Chapter 2: Change Management 2.1
Overview 2.1
Change Management High-level Process Description 2.1
Filtering Request for Change 2.1
Assessing the Impact of Change and Approval 2.2
Reviewing Changes 2.2
Closing the RFC 2.2
Change Management Process Flow 2.3
Roles and Responsibilities 2.4
Change authority 2.4
Change Manager 2.4
Caller or Requester 2.5
Change Initiator 2.5
Change Advisory Board and/or Technical Review Board 2.5
ECAB 2.6
CAB Meetings 2.6
Determining Type of Change: The Change Matrix 2.8

Exceptions to the Criteria 2.8
Request for Change (RFC) Form 2.9
Basic Information 2.9
Business Case 2.10
Costs (optional) 2.10
Schedule 2.10
Change, Test, and Backout, Plan 2.10
Approvers *(allows for changes to email notifications, as needed)* 2.11
Implementation 2.11
Post Review 2.11
Closure 2.12
Metrics 2.12
Monthly 2.12
Quarterly 2.12
Some Metric Guidelines 2.12
Training for ICS Change Management 2.13
Target Audiences 2.13
Syllabus (modify as needed for each audience) 2.13
Delivery Options for Training 2.13
Chapter 3: Problem Management 3.1
Overview 3.1
High-level Problem Management Narrative 3.1
Problem Management Process Flow 3.2
Roles and Responsibilities 3.3
Problem Management Review Team Roles and Responsibilities 3.3
Problem Manager 3.3
Tech Team Roles and Responsibilities 3.3
Cross-functional Team Roles and Responsibilities 3.4
Responsible Individual Role and Responsibilities 3.4
Inputs to the Problem Management Review Team 3.4
Known Problem Documentation 3.4
Prioritizing Problems 3.5
Problem Form 3.6
Schedule 3.6
Implementation 3.6
Closure 3.6
Problem Management Metrics 3.6

Training for ICS Problem Management....3.7
Target Audiences....3.7
Syllabus (modify as needed for each audience)....3.7
Delivery Options for Training....3.7
Chapter 4: Release Management....4.1
Overview....4.1
High-level Release Management Narrative....4.1
Major Release....4.1
Minor Release....4.1
Release Management Process Flow....4.2
Roles and Responsibilities....4.3
Release Manager....4.3
Build Developer....4.3
Acceptance Tester....4.3
Installer....4.3
Approval Authority....4.4
Release Planner....4.4
Determining Types of Release....4.4
Minor Release....4.4
Major Release....4.4
Components of the Release Plan Template....4.4
Closure....4.5
Metrics....4.5
Training for ICS Release Management....4.6
Target Audiences....4.6
Syllabus (modify as needed for each audience)....4.6
Delivery Options for Training....4.6
Chapter 5: Configuration Management....5.1
Overview....5.1
High-level Configuration Management Narrative....5.1
Configuration Management Process Flow....5.2
Input Trigger List....5.3
Versioning/Naming Conventions....5.3
Asset and CI Category Definitions....5.3
Type: Hardware....5.3
Type: Software....5.4
Type: Services....5.4

Type: Documentation 5.5
Example 5.5
Hierarchy Relationship Diagram 5.5
Auditing Requirements 5.6
Metrics 5.7
Training for Configuration Management Operations 5.8
Target Audiences 5.8
Syllabus 5.8
Delivery Options for training 5.8
Training Sources 5.8
Chapter 6: Asset Management 6.1
Overview 6.1
Asset Management – OCIO 6.1
Asset Management Procurement Process 6.2
Training for Asset Management Operations 6.3
Target Audiences 6.3
Syllabus 6.3
Delivery Options for training 6.3
Training Sources 6.3
Chapter 7: Capacity Management 7-1
Overview 7-1
Stakeholders 7-1
Activities 7-3
Data Gathering 7-3
ICS Server Hardware Capacity 7-4
ICS Database Hardware Capacity 7-4
Small Agencies 7-4
Networks 7-5
Capacity needs projections 7-5
Capacity Expansion Funding 7-5
Determining future needs 7-5
Capacity Needs Funding 7-6
Program Reviews 7-6
Capacity Reviews 7-6
Audits 7-6
Training 7-6
Chapter 8: Service Catalog 8-1

Overview 8-1
High-level Service Catalog Development Narrative 8-1
OCIO Service Catalog 8-2
Products and Services 8-2
Appendix A: Incident vs. Service Request vs. Change Request A-1
Appendix B: ITIL Acronyms B-1
Appendix C: ITIL Glossary of Terms C-1
Appendix D: Release Plan Template D-1
Appendix E: Capacity Management Data Gathering Graphical Samples E-1

Chapter 1: Incident Management

Overview

Definition of an incident: an unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Failure of a CI that has not yet impacted service is also an **incident**. For example, failure of one disk from a mirror set or of one node in a cluster would be incidents.

GOAL: The primary objective of Incident Management is to return the IT Service to users as quickly as possible.

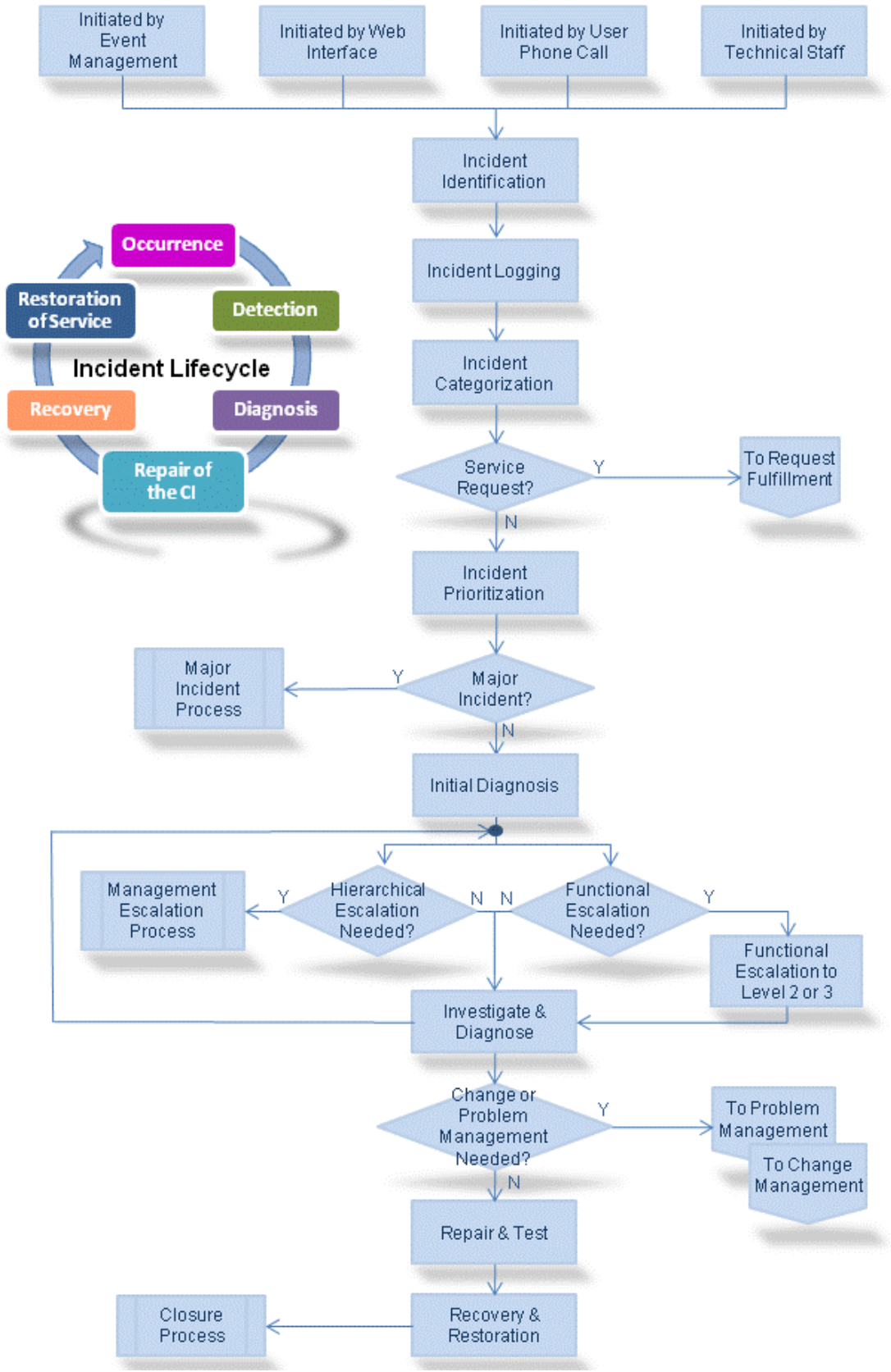
PURPOSE: **Incident Management** is the process responsible for managing the lifecycle of all incidents. It is designed to provide efficient methods for improving services to users, and to give IT services and service staff visibility.

Informally, if it was working before, and it is not working now, it is an incident.

High-level Incident Management Narrative

1. A user contacts Level 1 Support.
2. Level 1 Support records the pertinent information as determined by the Level 1 support organization, and determines the user's request is an incident. The incident will be categorized and prioritized. If it is a Major Incident, the Incident Manager will be notified.
3. Level 1 Support will try to resolve the incident. If the incident is resolved, the resolution is verified with user, documented, and the incident is closed. If the incident is not resolved, Level 1 Support requests assistance from Level 2 Support.
4. if the Level 1 Support request is received from outside OCIO, Level 2 support opens a new incident, records the pertinent information including any reference number from Level 1 Support in its Service Desk application. Level 2 tries to resolve the incident. If the incident is resolved, and the resolution is verified by the user through Level 1 Support, the resolution is documented and the ticket is closed. If the incident is not resolved, Level 2 requests assistance from Level 3 support. Status updates will be provided to the agency and/or user as agreed to in the Memorandum of Agreement (MOA) and determined by the incident urgency and priority.
5. As long as the incident remains unresolved, status updates will be provided to the agency and/or user as agreed to in the MOA and determined by the incident urgency and priority. Once the incident is resolved by Level 3 and verified by the user through Level 1 Support, the resolution is documented and the incident is closed.

Incident Management Process Flow



Roles and Responsibilities

Incident Owner: The service technician who is initially assigned to work on an incident. Ownership includes the responsibility to follow the incident's lifecycle through to closure.

Major Incident Team – A dynamically established team of IT managers and technical experts, usually under the leadership of the Incident Manager, formulated to concentrate on the resolution of a Major Incident.

Incident Manager – Leads the Major Incident Team and works to ensure that adequate resources and focus are provided to finding a swift resolution. The Incident Manager will also be the point of contact for communication during the Major Incident.

Support Levels Defined

Level 1 Support is responsible for the local environment to include, but not limited to, desktop, PDA/mobile device, network and server environments, as applicable. Level 1 support covers desktop applications and hardware, department specific software and management of user accounts.

Level 2 Support will be provided by the OCIO Service Desk, for purposes of the state's Consolidated Services.

Level 3 Support is considered to be Vendors and Consultants with maintenance or service contracts, or any 3rd party whose assistance is requested by the OCIO Service Desk to resolve an incident.

Incident Identification

Level 1 Support takes the call and determines if the request is an incident or service request following the guidelines in Incident vs. Service Request vs. Change Request. If this is a Service Request, logging and categorization are completed as for an incident, then it follows the agency's service fullfillment process.

Incident Logging and Preparation for Escalation to Level 2

Users at each agency should refer all incidents to their own service desk staff. Only Level 1 staff should determine which incidents should be escalated to Level 2, and only Level 1 technicians at each agency shall be designated as points of contact for these escalations. Once an incident is escalated, each agency's Level 1 staff shall maintain its chain of ownership, overseeing the incident process through to closure, including, but not limited to:

- ensuring responsiveness of Level 1 and Level 2 technicians in working toward resolution;
- facilitating any necessary communication between the user and Level 2;
- staying current with, and reporting the incident status to, the user; and
- following up on incident closure procedures.

All incidents must be fully logged and date/time stamped by a Level 1 technician at each agency so that a full historical record is maintained and relevant information is ready to hand to Level 2 support. Level 2 Support will be opening a new incident within their service desk with its own categorization and ID numbers.

Level 1 support should provide the following relevant information:

- a unique reference number for Level 2 to associate with its incident;
- the Level 1 categorization;
- incident urgency;
- incident impact;
- name of the person recording the incident, if different from the Level 1 designated contact (initial contact/Incident Owner);
- name of the Level 1 contact (this may be automatic based on Agency);
- name/department/phone/location (city/office/floor/room) of user;
- VIP status of user (is or is not a VIP);
- incident status;
- description of symptoms;
- if known, the related problem or known error; and
- steps already tried and the success or failure of the results.

Categorization

Incident Categorization is a vital part of incident development and documentation as it:

- helps a service technician search for an incident in order to reopen it, reuse its resolution for subsequent issues, or identify affected resources; and
- groups incidents into logical units for trending, and for reporting internally and to supported agencies.

Categorization is usually unique to each agency, so knowing and understanding these goals, as well as what trending and reporting needs an agency has, will help define the categories used. Each agency has the flexibility to set its own categories; when an incident is escalated to Level 2 it is subject to re-categorization by OCIO.

Some guidelines for categorization:

- Base categories on the service desk's business or service functions rather than on the business organization; organizational structure can change.
- Categories can be single- or multi-leveled; best practice is to go no more than 3- or 4- levels deep. For example:
- Category: Hardware
  Subcategory 1: Servers
  Subcategory 2: Public SQL Server

- For multi-levels use a top-down approach; level 1 should be the broadest category, with each subsequent level becoming more specific.
- Do not try to define the issue, such as “cannot connect to server” within the categories; this is described in the incident form’s short description or summary.

Setting Priorities

Priority is set by determining how urgent the incident is, and what its immediate impact is. Urgency is synonymous with how heavily work is impaired, while impact is synonymous with the number of people whose work is affected. Ugency and Impact can be set by selecting from drop down lists where the choices are assigned values, and priority can be calculated. Below are examples of the formulas used by OCIO. Resolution times are filled in based on MOAs developed with each agency. Priority may be changed upon escalation.

Formula: Impact + Urgency = Priority

Impact is to:	Me
	My Workgroup
	My Agency

Working Ability is:	Impaired
	Severly Impaired
	Stopped

			Urgency Working ability is:			Service Request
			Impaired	Severely Impaired	Stopped	
	Urgency Values →		3	1	0	7
Impact The impact is to:	Me	3	Low 3 + 3 = 6	Medium 1 + 3 = 4	High 0 + 3 = 3	Request
	My Workgroup	2	Low 3 + 2 = 5	High 1 + 2 = 3	Critical 0 + 2 = 2	Request
	My Agency	1	Medium 3 + 1 = 4	Critical 1 + 1 = 2	Major Incident 0 + 1 = 1	Request
	Impact values ↑					

Where:		Target Response Time:	Target Resolution Time:
Major Incident =	1	_____	_____
Critical =	2	_____	_____
High =	3	_____	_____
Medium =	4	_____	_____
Low =	5 or 6	_____	_____
All else =	7	_____	_____

Major Incident Process

Definition of a Major Incident - The highest category of Impact for an incident. A Major Incident results in significant disruption to the Business.

Once an incident has been prioritized as a Major Incident:

1. Based on circumstances, the CTO will designate an Incident Manager.
2. The Major Incident team will be assembled.
3. The Incident Manager will notify the appropriate parties by:
   a. status web pages,
   b. computer officers,
   c. e-mail distribution lists, or
   d. phone lists.
4. Once the team assembles under the direction of the Incident Manager, the team will work toward:
   a. identifying the cause of the incident,
   b. liaising with suppliers or maintenance providers,
   c. identifying and undertaking fix, and
   d. restoring service.
5. During this process the Incident Manager will be responsible for providing communication to stakeholders including, but not limited to:
   a. updates to action taken,
   b. requests to user actions such as applying security patches,
   c. estimated timelines, and
   d. releasing notification of a fix.
6. After the incident is closed the Incident Manager will again gather the team to discuss and identify:
   a. lessons learned,
   b. feedback to continuous improvement, and
   c. information to pass on to problem management.

Management Escalation Process

***Definition of Management Escalation* - T**he process that a Service Desk representative uses to notify management and stakeholders when an incident meets pre-defined criteria.

The following defines the criteria and steps needed for the Management Escalation Process.

- **Entrance Criteria:** An incident has been through the Incident Management Process Flow step of “Initial Diagnosis”.
- **Exit Criteria:** The Management Escalation Process has been completed and the incident has moved on to the step “Investigation & Diagnosis”

Management Escalation Criteria

The incident:

- is classified as a Major Incident, a Priority 1 or the Service Desk Representative deems that the situations warrants escalation, or
- cannot be responded too within the time specified in the MOA, or
- cannot be fixed within the specified time in the MOA, or
- affects the Executive Level category, or
- affects an entire agency.

Management Escalation Process

To escalate an incident to management, a Service Desk staff member:

1. Determines that the incident meets the criteria and needs to follow the Management Escalation Process.
2. Notifies the Service Desk Supervisor and follows OCIO escalation procedures.
3. Notifies the agency via phone of the plan to fix the problem and a specified time that the follow-up will occur.

Incident Closure

Incident closure is performed by the service desk. It is the final step in the Incident Management process and includes a number of activities.

Resolved incidents should be clearly documented to ensure:

- the steps taken to resolve the incident are defined;
- the incident is classified completely and accurately;
- resolution or action is communicated to the user to validate the user's requirements are satisfied. The incident may also be put in a RESOLVED state to give the user time to test or approve the resolution; an incident in a RESOLVED but not CLOSED state will auto close in 5 days; and
- time spent on the incident is recorded accurately.

Incident re-opening

In rare circumstances an incident can be re-opened. Incident re-opening should be defined in terms of metrics. A common example is that if an incident re-occurs within a 12 or 24 hour period then the original incident can be re-opened, otherwise a new incident must be logged.

Metrics

The best metrics emphasize outcomes and provide guidance about organizational goals. When metrics are designed correctly—and clear markers exist along the way—service staff understand what they need to accomplish. Understanding that more valuable metrics will become apparent over time, the following are provided as initial guidelines.

Metrics	Needed By: Ops Team	Customers	Steering Committee	What's Measured	Freq
Uptime % by Server	X			(Total Real Hours - Unscheduled Dow ntime - Scheduled Dow ntime)/(Total Real Hours-Scheduled Dow ntime)	Monthly
Uptime % - Average All Servers	X			(Total Real Hours - Unscheduled Dow ntime - Scheduled Dow ntime)/(Total Real Hours-Scheduled Dow ntime)	Monthly
CPU Utilization % - Average by Server	X			Utilized CPU/Available CPU	Monthly
Memory Utilization % - Average by Server	X			Utilized Memory/Available Memory	Monthly
Memory Utilization % - Average All Servers	X			Utilized Memory/Available Memory	Monthly
Disk Space Utilization % - Average by Server	X			Utilized Disk Space/Available Disk Space	Monthly
Disk Space Utilization % - Average All Servers	X			Utilized Disk Space/Available Disk Space	Monthly
Service Availability	X	X	X	dow ntime)	Monthly
Number of mailboxes by message store	X			Number of Mailboxes	Monthly
Number of mailboxes - all message stores	X			Number of Mailboxes	Monthly
Average message size by message store	X			Total Message space/Total number of mailboxes	Monthly
Average message size – all message stores	X			Total Message space/Total number of mailboxes	Monthly
White space (percent by message store)	X			Total unused space/ Total space	Monthly
White space (percent average – all message stores)	X			Total unused space/ Total space	Monthly
Total Unscheduled Dow ntime Hours	X	X	X	Dow ntime Hours	Monthly
Monthly Average Delivery Time	X	X	X		Monthly
Number of Incidents by Category for the agency	X	X	X	Number of Incident by Category	Monthly
Total Number of Calls per Agency	X	X	X	Total number of calls	Monthly
Number of Calls per Agency by Level	X	X	X	Number of calls by Level	Monthly
Number of Calls per Agency by Priority	X	X	X	Number of calls by Priority	Monthly
Number of Calls per Agency by Category	X	X	X	Number of calls by Category	Monthly
Number of Calls per Agency by requested date/time range	X	X	X	Number of calls by requested time/date	Monthly
Total Number of Calls All Agencies	X	X	X	Total number of calls	Monthly
Number of Calls All Agencies by Priority	X	X	X	Number of calls by Priority	Monthly
Number of Calls All Agencies by Category	X	X	X	Number of calls by Category	Monthly
Total Number of Major Incidents	X	X	X	Number of Major Incidents	Monthly
First Contact Response Times	X	X	X		Monthly
Time to resolve the incident after first contact	X	X	X		Monthly
Number of Calls Reopened	X	X	X	Number of calls reopened	Monthly
Responses to Customer Satisfaction Surveys	X	X	X	Responses to Survey	Monthly

Training for ICS Incident Management Operations

Target Audiences

- Level 1 techs
- Level 2 techs
- Users
- Owners
- Managers

Syllabus

- Purpose of Incident Management
- Common language
- Chain of Ownership
- Define levels
- Overview of processes
- How to implement processes in Service-now (OCIO only)
- Getting user information
- Incident assignments
- Types of escalation
- Passing information from Level 1 to 2 across agencies
- Roles and Responsibilities (who opens, who escalates, who set priorities, who resolves, who closes)
- Who is on notification list – moving level 1 tech to notification list
- Service Agreement

Metrics required

- What are the metrics?
- How to meet the metric requirements (associating incidents, closing, closing procedures)
- Priorities and Times: are changes needed? In OCIO? Between agencies?

Delivery Options for training

- Video Conference
- Phone Conference

Training sources

- HDI SCA course
- Operations meeting notes

Chapter 2: Change Management

Overview

Definition of a Change: Any action resulting in a new status or value in baseline or configuration data. (ITIL v.3)

GOAL: To reduce the amount of unplanned work as a percentage of total work done.

PURPOSE: To ensure planning, recognize what might be affected, monitor the effects of a change, quickly recover from failures, measure successes, plan training, and make all IT systems and CIs within an environment compatible and manageable, and to make changes visible within an organization.

Informally, a change is anything that affects the production environment. It may or may not include CI changes. Anything falling under this definition is subject to the change process. Incidents often neccessitate changes; a change usually begins as an incident.

Request for Change (RFC) is NOT the change, but is a formal proposal requesting the change. An RFC contains the reason for, and goal of, the change; the plan or steps and tasks for implementation; the backout plan; a proposed schedule; who will be affected; and any additional details of a change. RFC's can only be created by a service technician, never by a user.

Change Management High-level Process Description

Filtering Request for Change

The Change Initiator evaluates the issue to determine if its status should be Normal, Urgent, or Emergency, and creates an RFC, routes it and/or contacts the team lead based on the classifications below.

If Normal: The Request for Change is created and routed to the Change Manager to review for required information. The Change Manager then routes the RFC to the CAB for review and approval decision during the next CAB meeting.

If Urgent: The Request for Change is created and bypasses the CAB meeting. It is approved by the Change Initiator's team lead for appropriate implementation priority. The Request for Change is then sent to the CAB for review after the change has been implemented.

If Emergency: The team lead is contacted and approves implementation. The Request for Change is created after the change has been implemented and is then sent to the CAB for review.

Assessing the Impact of Change and Approval

The Change Advisory Board will review the RFC, and assess and rate its impact. If CAB has concerns or needs more information, the Change Manager and Change Initiator will work together to resolve issues. When no further issues are found, the CAB will make its approval decision.

Approved RFCs are assigned an implementation date determined by potential conflicts with other RFCs or business needs.

Reviewing Changes

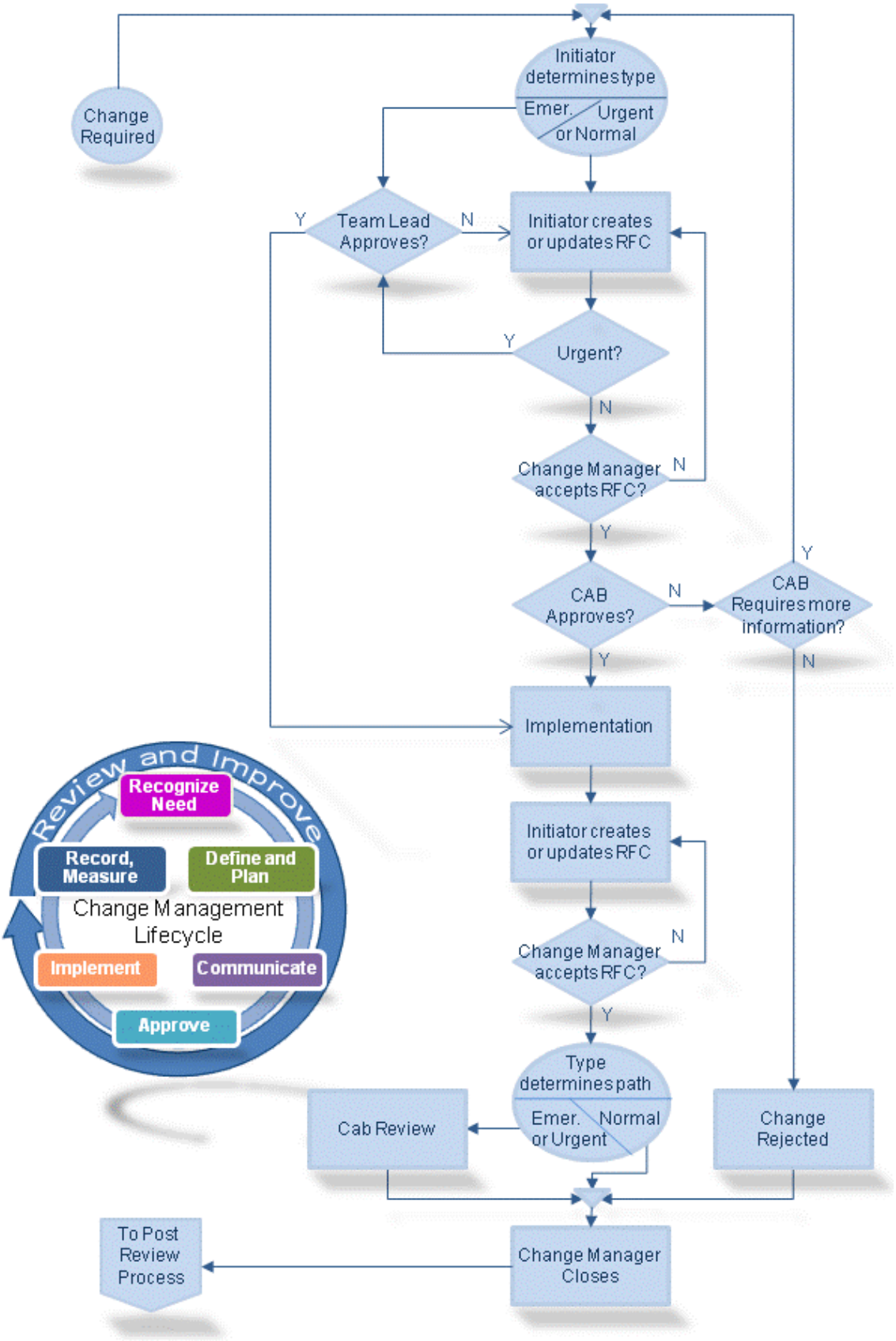
Once the RFC has been implemented, the Change Initiator completes the RFC post review and routes it to the Change Manager.

Closing the RFC

Once the RFC post review is completed the RFC is closed.

Note: Reviews of completed RFCs are managed through the metrics reporting done monthly and quarterly for the CAB or Review Board.

Change Management Process Flow



Roles and Responsibilities

Change authority

- Owns the change.
- Liaises through the Change Manager with technical teams and CAB.
- Reviews proposed changes, and authorizes or rejects each change.
- Can be the Change Advisory Board (CAB), Service Delivery Board, Technical Review Board (TRB), a person, or a Global Change Board.
- Oversees improvements to the process; ensures it is running correctly through regular review meetings (quarterly, semi-annually, etc.)

Change Manager

- Knows ITIL and IT.
- Is not necessarily a technical role.
- Oversees the process, making sure it is followed.
- Reviews RFCs for completeness, returns incomplete ones for further work.
- Decides on level of approval needed.
- Reviews RFC priorities and schedules meetings, making sure appropriate people are contacted based on expertise, nature of RFC or of needed change.
- Tables all RFCs for a CAB meeting, issues the agenda and circulates all RFCs to CAB members in advance of meetings to allow prior consideration.
- Chairs or mediates meetings.
- Convenes urgent CABs, assures approval.
- Receives change approvals from CABs and schedules notifications.
- Maintains the published Change Calendar and the Change Schedules.
- Liaises to coordinate change building, testing, and implementation between groups, when needed.
- Helps initiator meet schedules.
- Updates/Reviews change log to take opportunities to improve the service quality.
- Reviews completed changes to make sure they are closed properly, that SLAs are met, that change objectives are met, and refers back/reschedules backed out or failed plans, or makes sure they are moved to another management process.
- Reviews RFCs awaiting consideration or action.
- Analyzes change records to determine any trends or problems that occur; pursues rectification with relevant parties.
- Closes RFCs.
- Produces regular and accurate management reports.

Note: The Office of the CIO has committed to providing staff designated to fullfill the responsibilities of the Change Manager for State Enterprise Operations.

Caller or Requester

The person who submits a Service Request (which may include a request for some kind of change) or an incident that results in a change, is NOT the change requester. This person is the user. ***The change process begins when a Request for Change is created.***

Change Initiator

- Only a Service Technician can be a Change Initiator and propose that a change be made.
- Documents and devises required test and backout plans.
- Fills out and submits the RFC, including requested schedules; needs descriptions; change, backout and test plans; associated incidents; risks; anticipated problems and tasks; who and what will be affected.
- Plans change schedule based on when the next CAB meeting is scheduled and when the next maintenance window will be.
- Executes the change (may oversee a change team but actually participates in the work the change requires) including all testing, and reporting of results to the Change Manager.
- Updates the change tasks.
- Updates associated CI change documentation.
- Makes sure the change history is accurate – all documentation is complete with accurate dates on when changes are implemented (go live).

Change Advisory Board and/or Technical Review Board

- The CAB supports the authorization of changes.
- Best model meets at least weekly; these meetings can take 15 minutes to an hour depending on the maturity of the process.
- Assesses and prioritizes changes submitted to it through RFCs.
- Fleshes out request for change, if needed.
- Moves the change to the release management process (scheduling; may be an ad hoc or a formal process).
- Consists of those with decision-making authority, and the ability to assess changes within the scope of the CAB from a business and a technical viewpoint.
- Includes the Change Manager.
- May be asked to recommend adoption or rejection of changes, then submit those recommendations to a higher-level change authority.
- May authorize changes.
- May delegate the responsibility of authorizing changes (as a CAB with change authority allowing a technical review team to actual authorize a change).
- Sets the minimum time before a change can be implemented.
- Ensures emergency changes are documented.
- Could potentially include:
- The customer
- The user manager

- Applications developers or maintainers
- Technical consultants
- Services and operations staff: service desk, test, security, and/or capacity managers
- Facilities staff
- Contractors where outsourcing is necessary
- Marketing, police (traffic disruptions), financial services…
- Will be composed according to the changes being considered .
- May vary over the course of a single meeting.
- Should involve suppliers when that would be useful.
- Should represent both users' and customers' views.
- Might include the problem manager and service level manager, and user relations staff (human resources).

ECAB

- This body is small and has authority to make emergency decisions.
- Change procedures should specify how the composition of the ECAB will be determined in each instance; this is for flexibility, and to represent business interests properly.
- Should be designed to make decisions in any eventuality from a business and technical standpoint.
- Staff knows who the members of the ECAB are at all times.

Recommendation: a CAB should have stated evaluation criteria which will act as a template for assessing changes (can be developed by the ITIL Change Management Team).

CAB Meetings

We should consider that our CABs may be across agencies or other state or consulting entities, and use an Open Model**,** where:

- meetings do not need to be face-to-face;
- electronic or e-supported phone or video conferencing should be considered;
- meetings are on set schedules, attended by the core staff and any invitees;
- meeting schedules, attendance information, and subjects (RFCs) are published so that any agency can have a representative attend, in person or electronically, if they feel they may be affected by the change; and
- face-to-faces need to be planned to the majority's advantage: parking, time, room size…

Recommendation: Regularly scheduled meetings (weekly) with electronic support work best.

Weekly meetings should be used to:

- focus on changes only;
- discuss and sign-off on changes that have been disseminated to CAB members;
- review outstanding changes; and
- discuss major upcoming changes

Cab Meetings should have a standard agenda and may include:

- RFCs to be assessed, in priority order;
- RFCs that have been assessed and require further discussion;
- scheduling of changes and schedule updates;
- change reviews;
- outstanding changes;
- failed changes reviews;
- advance notice of RFCs to be reviewed at the next CAB; and
- review of unauthorized changes and decisions about remediation.

To reduce meeting time, RFCs and relevant documents should be circulated in advance to:

- speed up meetings;
- allow necessary resource and impact assessments to be made; and
- allow Cab members to delegate a deputy or send comments.

Quarterly Review Meetings should be used to:

- make amendments to the process;
- review;
- accomplishments and business benefits;
- metrics;
- users and surveys;
- programs; or
- failures/improvements.

Determining Type of Change: The Change Matrix

	Criteria	Approval	Documentation Required
Normal	Changes that must be performed in order to correct or improve service having some impact on customer's business. Impact to business does not warrant immediate or urgent correction	Change Advisory Board	Request for Change forms completed before change is evaluated within the guidelines of the CAB.
Urgent	Changes that must be performed in order to correct a faulty IT service having an immediate Impact on the customer's business. Impact to business requires immediate resolution	Team Lead	Request for Change forms completed before change is evaluated.
Emergency	Only to repair an error in an IT service that is negatively impacting the business to a high degree.	Team Lead	Request for Change forms must be submitted within one business day of change being made.
Policy Violation	Changes that have been implemented without going through the change process.		RFC is marked for review by the CAB

Exceptions to the Criteria

These exceptions should be entered as Service Requests, incidents, or Maintenance items.

- Changes in setting-up, deleting or modifying user accounts to include setting passwords, system configuration changes and managing licenses to allow user access.
- Setting up and configuring maintenance/monitoring systems to include configuration changes and IP addresses.
- Changes to descriptions, data elements that appear on screens or reports to include messages, data updates to tables and systems/programs parameters. Exception to this would be a program or script which would perform mass updates in production.
- Changes to single user equipment ie PCs/Phones and single user software installation/updates.
- Change out of hot swappable infrastructure components.
- Routine system maintenance activities ie Server reboot/system backups/ vendor software updates not requiring Release Management/database compressions. With the exception of server reboots, these activities typically do not require system downtime. Backup schedule changes do not need to be approved unless the backup window changes.
- Content updates of static pages or documentation.

Request for Change (RFC) Form

The listed form fields comprise information needed for a complete RFC. The RFC is divided into sections of related information to focus thought processes. Bullets indicate selection items or choice lists to reduce RFC development time and form space. Basic form and fields may be implemented in each Agency's Service Desk software, and reflects the minimum information needed.

Basic Information

Change Number (Auto):	Reference Number:
Assigned To :	CI to be changed: *(if available)*
Status: • Open • Pending • Work in Progress • In Review • On Hold	Change Type: • Normal • Urgent • Emergency
Priority : • Low • Moderate • High • Critical	Risk : • Low • Moderate • High • Very High
Category: • Business Service • Network • Documentation • Etc.	Approval : • Not Yet Requested • Requested • Approved • Rejected • Policy Violation
Title: (text)	

Business Case

Change Description	
Change Justification	
Impact of No Change	
Benefit Is To: • Enterprise • Multiple Agencies • Agency • Division • Staff	Stakeholders: *(list of people or groups to receive notifications)*

Costs (optional)

Cost Types:	Cost Status:
☑ Normal Operations ☐ Contractor Bid ☐ Software Purchase ☐ Hardware Purchase ☐ Intangible Asset (GASB)	• Requesting Analysis • Analysis Approved • In Progress • In CAB Review • Cost Approved • Cost Denied • Not Applicable
Approx. Cost to Adopt Change: $	

Schedule

Requested By Date:	Actual Start:
Planned Start Date:	Actual End:
Planned End Date:	Actual Manhours:

Change, Test, and Backout, Plan

Change Plan:
Test Plan:
Backout Plan:

Approvers *(allows for changes to email notifications, as needed)*

Select Approver:
- CAB
- Team Lead 1
- Team Lead 2

Etc.

Implementation

Work Log: *(on-going log or journal of work done)*

Post Review

Closure Code – the change: • Was Successful • Was Canceled • Had Unexpected Outcome • Required Back Out	Briefly explain cancellation, unexpected outcome, or reason for backout:
Move to: • None • Incident Management • Project Management • Knowledge Management • Problem Management	Briefly explain reason for move:
Training Required: • None • One-time • On-going	Training Notes:
Confirm: ☐ Change Documentation Complete ☐ Operations Documentation Complete ☐CMDB Updated *(if available) (on-going maintenance, training, etc.)*	
Request further actions: ☐ Make this a KB Item ☐ Request Quarterly CAB Review	
Lessons Learned *(for improvement cycle):*	

Closure

Once the change has been approved and implemented, cancelled, or backed out, the Change Initiator completes the Post Review, and the Change Manager closes the RFC.

Metrics

Suggested metrics for Change Management are:

Monthly

- Changes by Type of Change
- Unsuccessful Changes
- Successful Changes
- Reports by category based on importance to the organization (security, infrastructure, etc.)

Quarterly

- Counts by Change Type
- Trends Analysis by Change Type (are # of changes going down or up, for example)
- Changes by Category

Some Metric Guidelines

- Normal changes should make up about 90% of the total changes.
- Urgent changes should make up about 10% of the total changes, at most. Too many indicate areas for review as to why they are happening. Initially this may be due to a lack of understanding about the change process.
- Emergency changes should occur seldomly, one to 4 per year.

Once you hit a balance in your process, watch for imbalances as indicators that attention is needed. At this point, however, your main focus can move elsewhere.

Training for ICS Change Management

Target Audiences

- CAB members
- Change Managers
- Change Initiators
- OCIO IT Staff
- Agencies' Service Desk Staff

Syllabus (modify as needed for each audience)

- Goal and Purpose of Change Management
- Definition of a Change
- Maturation Process
- Common Language (including ITIL wording and common wording)
- Change vs. Service Request vs. Incident
- Chain of Ownership
- Roles and Responsibilities (who opens, reviews, updates, approves, schedules & prioritizes, manages notifications, documents, closes, final review)
- Types of changes
- High-level Process Description and Flow
- Requirements for RFC
- Implementing Processes in Service Desk Tools
- Notifications
- Calendars
- Scheduling changes – Based On:
- CAB meetings
- Maintenance Windows
- Stakeholder Notices
- Closing Processes
- Post Implementation Review
- Service Agreement
- Metrics Required
- How to prepare for and meet metrics requirements

Delivery Options for Training

- Video Conference
- Phone Conference
- Online Course
- Training Sources
- ITD Training Presentation
- Operations Meeting Notes

Chapter 3: Problem Management

Overview

Definition of a Problem: A cause of one or more incidents, or an incident whose cause is not known. The Problem Management Process is responsible for further investigation. (ITIL v.3)

GOAL: In order to reduce user issues and produce repeatable, predictable results, the primary objective of Problem Management (PM) is to make problem resolution a priority.

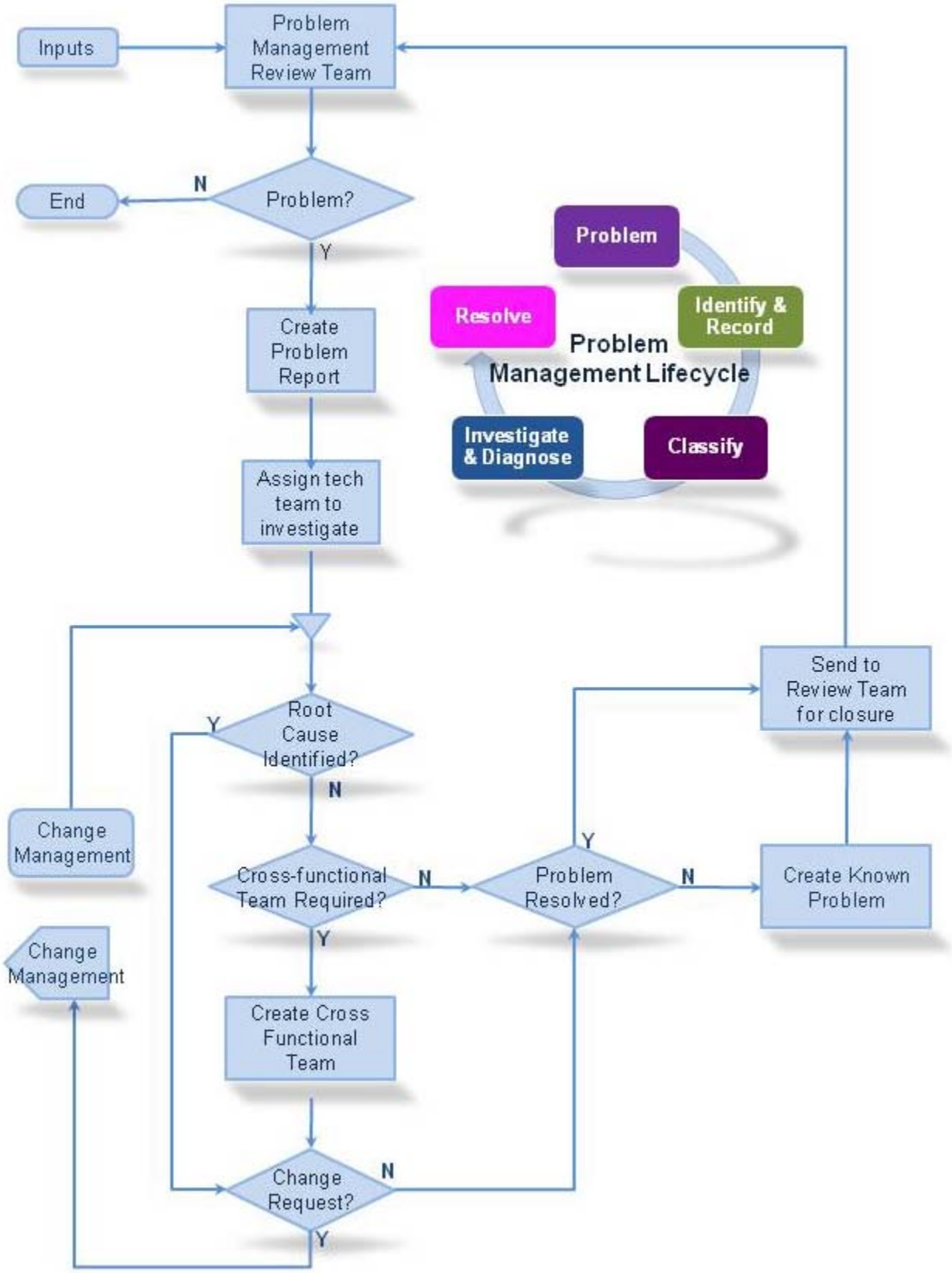
PURPOSE: Problem Management seeks to get to the root cause of incidents and then initiate actions to improve or correct the situation

The first priority before beginning Problem Management is to get any affected IT services back online through the Incident Management Process. Once this is done, the Problem Management process allows service technicians to take the time necessary to gather information, evaluate, identify, and diagnose the root cause of the problem.

High-level Problem Management Narrative

1. A service technician determines that an issue requires an analysis to determine its cause, and requests review by the Problem Management Review team.
2. If the team agrees that the issue is a problem, it ceates a problem report, assigns a Problem Manager, and selects staff for the Tech Team. The Problem Manager assigns the Responsible Individual to lead the tech team in researching for a root cause. Documentation is ongoing through the life of the problem.
3. The tech team begins research to determine a root cause. They may decide they require expertise outside of their specialty and request the Problem Management Review team create a cross-functional team. In either case, the team:
   - resolves the problem;
   - creates a change request; or
   - decides the problem cannot be resolved and creates a known problem report.
4. The report is sent to the Review Team for follow-up or closure.

Problem Management Process Flow



Roles and Responsibilities

Problem Management Review Team Roles and Responsibilities

A Problem Management Review Team (Review Team) seeks to cure the causes of problems. It reviews reports and trends of incidents that have already occurred in order to identify and record problems. They receive information about reported incidents from the Incident Management process, service desk, or external sources. Members of this team:

- analyze this information, looking for similarities in the symptoms of reported incidents;
- look for records of previously identified problems that can explain the symptoms;
- ensure a record describing a new problem is created, if no resolution can be found; and
- review open problems until each is resolved, ensure each is ready to close, close each.

Problem Manager

The Problem Manager leads the review team in an administrative capacity. Assignments, decisions, and task directions given by this role are done under the direction of the review team. This role does not need to be a technical expert; it is assigned to one who:

- understands and oversees the process, making sure it is followed;
- reviews the problem report to ensure complete information/documentation exists;
- assigns problem to the appropriate technical team;
- assembles Cross-functional teams and schedules meetings;
- contacts the appropriate people based on expertise and the nature of the problem;
- facilitates/mediates Cross-functional team meetings;
- ensures requests for change are submitted and completed, if required;
- ensures known problems are accurately created and are complete;
- closes problem reports after final review by the Review Team; and
- produces regular and accurate management reports.

Tech Team Roles and Responsibilities

The Tech Team is made up of subject matter experts from one functional area or technical department; i.e. Network Support, Desktop Hardware Support, etc. They perform the required tasks and search for a resolution to problems by:

- analyzing known information;
- searching for the root cause of the problem;
- searching for a solution that will eliminate the root cause of the problem;
- closing the problem report upon resolution; and
- creating a **Known Problem** record with available workarounds, if no solution is found.

The Tech Team resolves the majority of problems. If the root cause or resolution is not found because the problem is outside the scope of the Tech Team, a Cross-functional Team may be formed to look at the problem. This team is formed by exception only.

Cross-functional Team Roles and Responsibilities

The Cross-functional team consists of relevant members with different functional expertise in the group's targeted issue. It is organized as needed and then disbands. The team uses a wide range of information to diagnose and resolve a problem. Representative team members are typically individuals from help desks, desktop hardware support, desktop software support, network support, operations support, applications support, server support, database administration, development groups, key user groups, and external suppliers. A Problem Manager facilitates and sets clear direction and purpose, assigns tasks, and makes decisions. Typical duties include:

- accessing upper management;
- brainstorming the problem, collective problem-solving and experimentation;
- identifying and prioritizing requirements by severity, impact, urgency, and risk;
- acquiring a team consensus as to a requirement's inclusion and priority; and
- all duties of the Tech Team.

Responsible Individual Role and Responsibilities

The Responsible Individual is the member of the Tech Team or Cross-functional Team to whom the Problem Manager assigns the lead role in researching and resolving an identified problem. There will be only one Responsible Individual at a time. If a problem is escalated to a Cross-functional Team, the role may be assigned to a different person. Typical duties include:

- ensuring all resources of the team are applied to resolving the problem;
- updating the problem ticket; and
- notifying the Problem Manager of the outcome.

Inputs to the Problem Management Review Team

Sources of information on problems include:

- Copies of Major Incident reports.
- Inputs from internal and external sources, ie., service techs, managers, users, etc.
- Incident Management Trend reports to include:
- Top 10 Incident count for 6 months for each Priority, by Category.
- Incidents without resolution for 3 months.
- Top 10 Incident count by Agency.

Known Problem Documentation

When there is a known problem, it needs to be recorded in a database until it can be resolved. For OCIO, these will be held in the Knowledge Base. The data recorded should include:

- details of the problem;
- symptoms associated with the problem;
- any workaround(s) in place;
- reference numbers and a count of related Incidents; and
- reason for no permanent solution (cost, bug, scheduling, future software release, etc.).

Prioritizing Problems

Establishing priorities for problems is more complex than prioritizing incidents. Problem priorities are based on impact and urgency the same as incident priorities, but are also influenced by other factors that must be considered by the lead technician or problem management review team on a case by case basis. The following should be considered when setting problem priorities.

Factors	Description	Situational influences
Impact	How many people are affected?	One person, a workgroup, or an agency
Urgency	Has the immediate need been resolved through Change or Incident Management?	If a workaround is in place, users can get work done until the root cause is found and fixed.
Frequency	How many incidents are believed to be related to this problem?	Calculate hours of impairment or down time: 10 incidents for 1 person = 1 incident for 10 people = 10 hours of impaired or stopped work
Risk	What is the risk of the problem causing additional incidents?	The goal is to reduce potential risks.
Resources	When will staff be available with the skills to research and resolve?	Resource availability is dependent on what other priorities exist, and what influences access. It may result in a lower priority, or a resource shift.
	When will equipment be available? Is resolution dependent on software releases, vendor availability, or other outside time frames?	Coupled with costs and scheduling, these may be beyond Problem Team controls, and must be relayed to the user as a delaying influence.
Cost	Will additional costs be incurred that need to be approved? If a vendor or consultant is involved: What is their fee? Are we eligible for updates or must a contract be put in place?	Once a root cause is known, cost may drive status and/or scheduling and delay problem resolution. The Problem Management Review Team may lower the current priority; change the status to On Hold; close the problem open or keep it open; or, establish some other course of action and tracking appropriate for its agency. In any case, a Known Problem report should be created.
Severity	Can the system be recovered, or does it need to be replaced? How many CIs are affected? How long will the fix take?	The seriousness of the problem from an infrastructure perspective should be determined. If numerous CIs are affected, the severity may increase requiring a higher priority. Time required for resolution will affect priority, depending on the severity and resources.

Problem Form

Problem Number (Auto): Assigned To :	Related Incidents: ***(allow multiples)***
Status: • Open • Pending Change • On Hold • Known Error • Pending Closure • Closed/Resolved	Related RFC: CI to be changed: ***(if available)*** Escalate to cross-functional team: ☐ Yes ☐ No
Priority : ☐ Low ☐ Moderate ☐ High ☐ Critical	Category: • Business Service • Network • Documentation Etc.
Title: (short description)	

Schedule

Resolution Due Date:	Actual Start Date:
Actual Resolution Date:	Actual Manhours:

Implementation

Description:
Work Log:

Closure

Resolution/Recommendation:	
Move to: ☐ Change Management	☐ Knowledge Base (as a "Known Problem" with workaround solution)

Problem Management Metrics

- How many problems have been identified and removed from the environment?
- How many problems have a status of resolved and closed?

Training for ICS Problem Management

Target Audiences

- Level 2 Service Desk Staff
- Problem Managers
- Service Desk Staff who may be considered as Responsible Individuals
- OCIO Team Leads
- Agencies' Lead Staff

Syllabus (modify as needed for each audience)

- Goal and Purpose of Problem Management
- Maturation Process
- Roles and Responsibilities (who opens, reviews, updates, approves, schedules & prioritizes, manages notifications, documents, closes, final review)
- Team Techniques for brainstorming, evaluating
- Process Description and Flow
- Implementing Processes in Service Desk Tools
- Collecting Input
- Requirements for Review
- Stakeholder Notices
- Closing Processes
- Metrics Required

Delivery Options for Training

- Video Conference
- Phone Conference
- Online Course
- Operations Meeting Notes

Chapter 4: Release Management

Overview

Definition of a Release: A collection of hardware, software, documentation, processes or other components required to implement one or more approved changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity. (ITIL v.3)

GOAL: The goals of Release Management include:

- Planning the rollout of software
- Designing and implementing procedures for the distribution and installation of changes to IT systems
- Effectively communicating and managing expectations of the customer during the planning and rollout of new releases
- Controlling the distribution and installation of changes to IT systems

PURPOSE: Release management focuses on the protection of the live environment and its services through the use of formal procedures and checks.

High-level Release Management Narrative

First, determine the release strategy that is most appropriate depending primarily on the size and impact of the release. The two types of releases are Major and Minor.

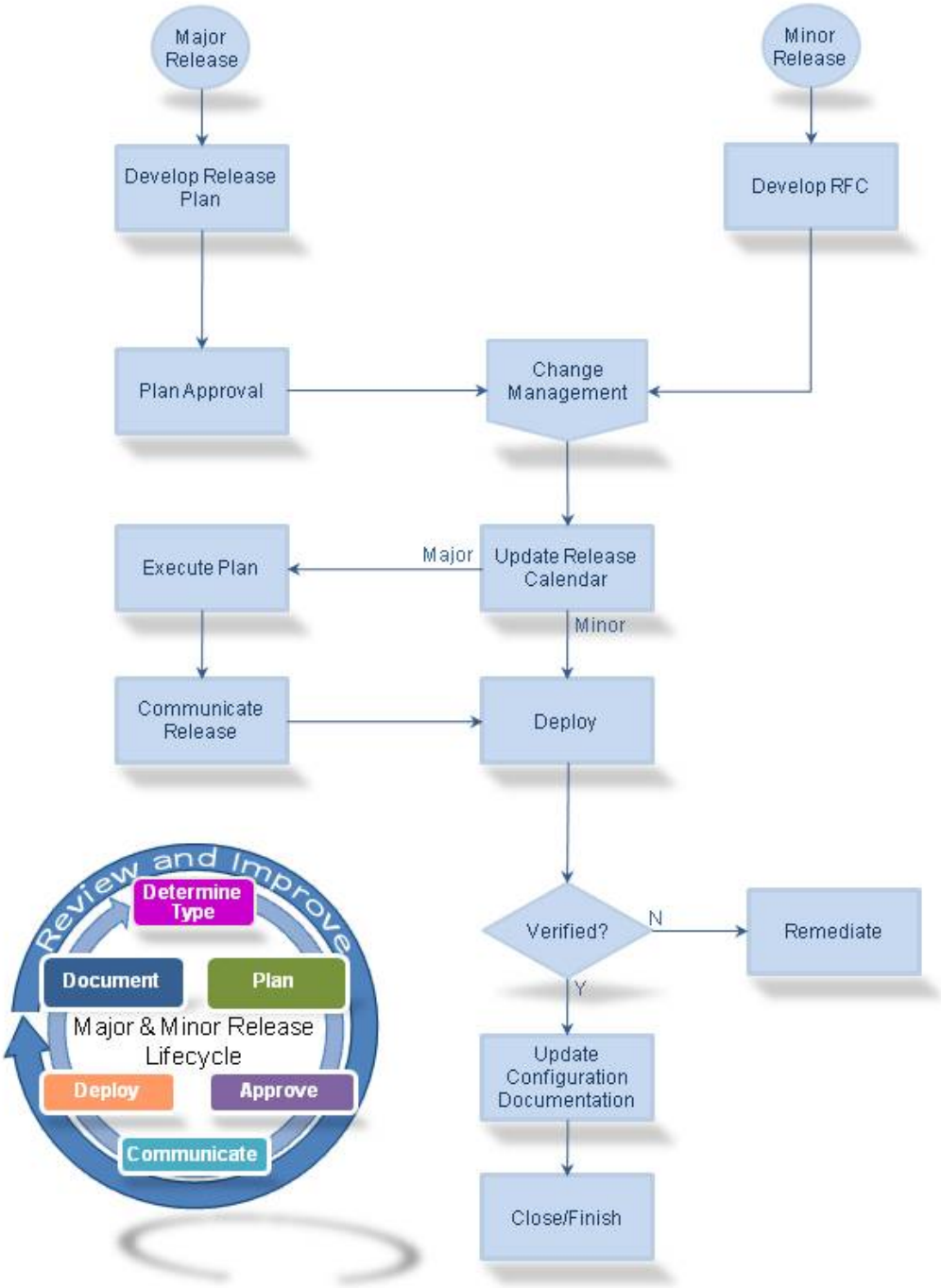
Major Release

1. Typically associated with project activities, a major release will require a release plan. A template can be found in Appendix D: Release Plan Template. The release plan brings together the key elements of the project management process necessary for planning a successful implementation of an IT system.
2. Once a release plan has been approved, the release is entered into the Release Calendar.
3. The approved release plan is executed and appropriate communications are made.
4. Once all changes have been verified and any issues resolved, they are entered into appropriate configuration documentation and the release is closed.

Minor Release

1. The change management process steps are sufficient for successfully planning a minor release into the production environment.
2. Once a Request for Change (RFC) or Maintenance item has been approved, the release is entered into the Release Calendar.
3. The change is deployed and the RFC is completed.
4. Once all changes have been verified and any issues resolved, they are entered into appropriate configuration documentation and the release is closed.

Release Management Process Flow



Roles and Responsibilities

Release Manager

- Is responsible for Release Management and ensuring that the process is followed
- Is the process owner
- Should have some understanding of the hardware and software deployed
- Does not need to be very technical
- May be the person responsible for ICT and/or technical support
- Some or all activities may be delegated to a technician

Build Developer

- Creates new builds
- Tests the stability of new builds and resolves any issues
- Tests the impact of new services on existing components of the build and resolves any issues
- Creates build procedures for all new hardware and software installation
- Stores software in the definitive software library
- Stores technical and user documentation appropriately
- Liaises with acceptance testers to ensure service functionality
- Ensures that installers are aware of new build procedures
- Supports installers in the event of difficulties installing a product
- Must be a technical person

Acceptance Tester

- Tests the functionality of new hardware and software
- Takes the user perspective on whether the product does what it was intended to do
- Liaises with the build developer to agree test criteria and perform tests
- Does not need to be technical
- Must be familiar with the requirements of the product being tested
- Is likely to be an end-user

Installer

- Installs new equipment in response to user requests
- Must use the install build checklist and the appropriate build procedure to execute all installations
- Liaises with build developer for assistance if necessary
- Refers any issues with build procedures to build developer or release manager
- Will be a technical person
- Will probably be involved in day-to-day Incident Management

Approval Authority

- Approves/Disapproves proposed releases
- Provides necessary resources to complete release
- Likely to be the CAB

Release Planner

- Completes Release Plan

Determining Types of Release

Minor Release

When an RFC is adequate to make the change and a Release Plan is not needed, it is considered to be a minor release. Staff training is not needed. A support plan is not needed. End-user or system support documentation does not require an update.

Examples of Minor Releases:

- Routine Patches
- Change has little impact to the end-user
- An enhancement or modification to something already existing
- Resolution to an incident
- RFC is adequate for planning
- Routine and/or repetitive tasks (such as standing up a new server)
- Changes to a routine/repetitive RFC already in place (such as a change to the timeframe of the maintenance window used)

Major Release

When a service is changed or a new service is introduced that requires such processes as planning, designing, building, testing, training, communications and deployment activities. It is considered to be a major release when the project/task is not routine, is complex enough to require a Release Plan, has impact to the end-user and/or support team.

Examples of a Major Release:

- Development of a new application
- Version update with enhancements and/or substantial changes to an existing software application
- New technology adoption
- A change to a business process that impacts the end-user or support team

Components of the Release Plan Template

- Release Plan Overview
- Risk Plan
- Support Plan

- Communication Plan
- Test Plan
- Training Plan
- Finish/Closing Plan

For a complete template see Appendix D: Release Plan Template.

Closure

Once the release has been approved, implemented, and verified, the Release Manager ensures the configuration documentation is updated, any issues are tracked and resolved, and lessons learned are documented.

Metrics

Suggested metrics for Release Management are:

Quarterly

- Number of releases by Type (Major, Minor)
- Number of releases by Type then by Category
- Successful Releases
- Unsuccessful Releases

Training for ICS Release Management

Target Audiences

- Level 2 Service Desk Staff
- Release Managers
- OCIO Team Leads
- Agencies' Lead Staff

Syllabus (modify as needed for each audience)

- Goal and Purpose of Release Management
- Definition of Release
- Maturation Process
- Roles and Responsibilities
- Types of Release
- Process Description and Flow
- Implementing Processes in Service Desk Tools
- Calendars
- Stakeholder Notices
- Metrics Required
- Closing Processes

Delivery Options for Training

- Video Conference
- Phone Conference
- Online Course
- Operations Meeting Notes
-

Chapter 5: Configuration Management

Overview

Definition of Configuration Management: The process responsible for maintaining information about configuration items (CI) required to deliver an IT service, including their relationships. This information is managed throughout the lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.

GOAL: The goals of Configuration Management include:

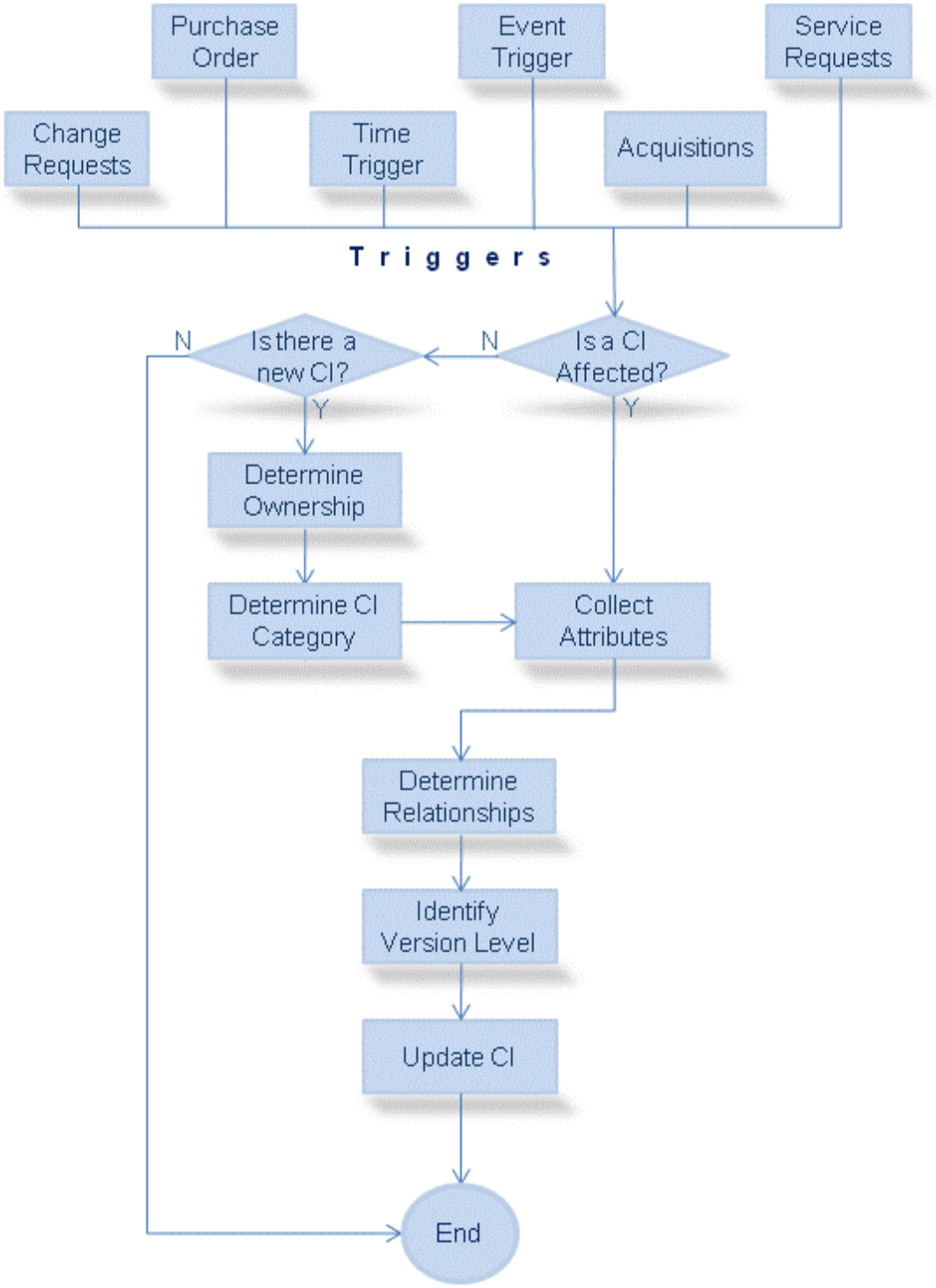
- Provide accurate configuration information to enable decisions at the right time supporting change, release, incident and problem management processes.
- Optimize assets, configurations, capabilities and resources.

PURPOSE: Define and control the components of services and infrastructure and maintain accurate configuration information on the historical, planned and current state of services and infrastructure.

High-level Configuration Management Narrative

Certain events will trigger a change to the current configuration as documented in the Configuration Management Data Base (CMDB). The effected configuration item (CI) will be identified, or created if necessary, and the appropriate attributes of the new configuration will be collected. Additionally, the relationships of the CI to other CIs will be determined. The appropriate version level of the new configuration will be determined and the collected information will be used to update the CI in the CMDB.

Configuration Management Process Flow



Input Trigger List

The following triggers will engage the configuration management process:

- Change requests
- Purchase orders
- Acquisitions
- Service requests
- Event Trigger – Any change on Configuration Management relevant CI (Type) or Relation (Type) is only triggered by the Change Management process
- Time Trigger - continual audits may change the status of a CI Type

Versioning/Naming Conventions

In order to maintain consistency and reduce confusion, the version of a CI will be the same as identified by the appropriate vendor. Additionally, the ICS Standard Naming Conventions will be used for identifying specific assets within the CMDB. These are found at: http://cio.idaho.gov/pdf/messaging_naming_conventions_guidelines.pdf.

Asset and CI Category Definitions

Type: Hardware

CLASSES

- Desktop/Laptop
- Server
- Appliances (security, other)
- Networking Equipment
- Telephone systems
- Printer
- Scanner
- Cell phone
- PDA

CONFIGURATION ITEMS (CI)

- Manufacturer's given name of the hardware followed by the ICS standard naming convention of agency code, location, and function information. Example: Dell PowerEdge 2650-ADMBOIDC
- Function (file, print, web, database, DNS, DHCP, Backup, firewall, VPN, IPS, IDS, Spam control, Virus control, switch, router)
- Responsible owner

ATTRIBUTES

- System components
- Location of equipment
- Equipment owner
- Topology
- Warranty

Type: Software

Classes

- Operating System
- Database
- Web Server
- Virtual server
- Productivity Suite
- Applications
- Messaging

Configuration Items (CI)

- Manufacturer's given name of the software
- Software owner

Attributes

- Version
- Location of software media
- number of licenses
- license keys
- Warranty
- Updates, patches applied

Type: Services

Classes

- Internet Service
- Telecommunication circuits
- Service Agreements
- Lease Agreements
- Hosting Services

Configuration Items (CI)

- Name of Provider
- Terms of service or agreement
- Type of circuit (fiber, copper)
- Type of lease

Attributes

- Bandwidth size
- Location of circuits
- class of circuit (FRS, ATM, P-to-P)
- Type of fiber (single-mode, multi-mode)

Type: Documentation

CLASS

- Statutes
- Standards, Policies, Guidelines
- Systems, software manuals
- Training related documentation
- Desk manuals

CONFIGURATION ITEM (CI)

- Document Title
- Date of last revision
- Originating organization

ATTRIBUTES

- Location
- Media (i.e. Hardcopy, Electronic)
- Meta Data (i.e. description of the document, keywords)
- Type of file (i.e. Excel, Word, PDF, PowerPoint)

Example

Type: Hardware → Class: Server → CI: Dell PowerEdge 2650-ADMBOIDC → Attributes: Rack Mount, 2U
2.3 GHz Intel CPU
6Gb RAM
RAID 5

Note: In the above example the Configuration Item (CI) incorporates the manufacturer's given name of the hardware and the ICS Standard Naming Conventions. The server is a Dell PowerEdge 2650 belonging to the Department of Administration and its function is a Domain controller.

Disclaimer – This section, "Asset and CI Category Definitions," is included in this chapter as a guideline. Since CMBD products may present their CI-related information differently it may not directly relate to the specifications provided in this section.

Hierarchy Relationship Diagram

The purpose of CMDB relationship hierarchies is to quickly identify related CIs that might be affected when one CI is having issues or goes out of service. Hierarchies are built from a service perspective rather than from business processes; they should help manage availability of service as defined by users.

There are three parts to a relationship hierarchy. These are the:

1. the first half of a relationship, which is a CI;
2. the type of relationship;
3. the second half of the relationship, which is a CI, a user, or a group

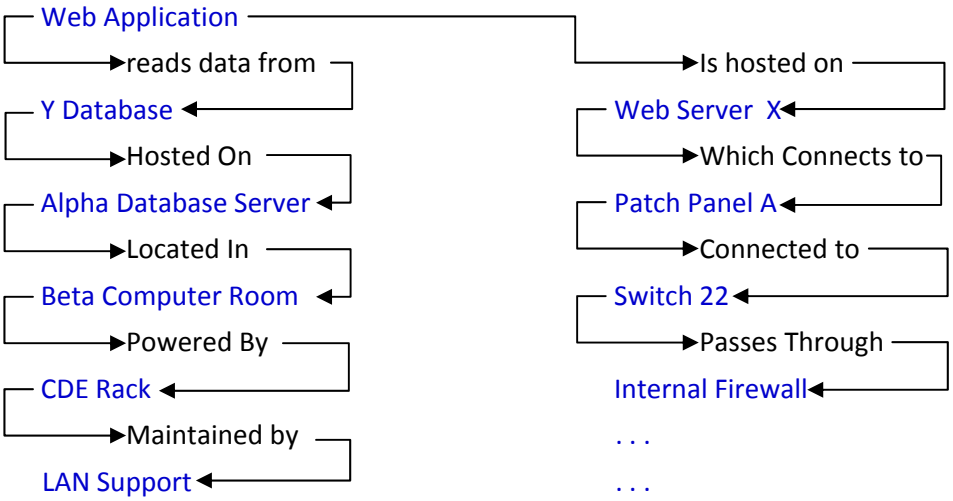
The "type of relationship" is the tie that binds the first and second half of the hierarchy. What follows is a list of suggested types of relationships, but it is not exhaustive:

- Connected to :: Connected by
- Depends on :: Used by
- Hosted on :: Hosts
- Instantiates :: Instance of
- Members :: Member of
- Rack contains :: In Rack
- Virtualized by :: Virtualizes
- Contains :: Contained by
- Exchanges data with
- Houses :: Is housed by
- IP Connection
- Powers :: Powered by
- Receives data from :: Sends data to
- Zone contains :: Located in Zone

Tying the two parts together with a type gives us a hierarchy relationship, for example:

1. CI to CI; ex: a computer connected to a printer;
2. CI to user; ex: a computer used by Jon Doe
3. CI to Groups; ex: a computer backed up by User Support Group

Hierarchies can be joined together by additional types to get streams of hierarchical relationships:



Auditing Requirements

Configuration management auditing will be completed by staff within the Office of the CIO.

Auditing in this regard will not consist of a complete comprehensive audit of an entire CMDB due to the time and resources it would require. An audit will consist of the below verifications on randomly selected items or when there is detection of any unauthorized CIs or changes having been made.

- Verify there is conformity between the documented baselines (e.g. agreements, interface control documents) and the actual business environment to which they refer.
- Verify the physical existence of CIs, the functional and operational characteristics of CIs, and check that the records in the CMS match the physical infrastructure.
- Verify that release and configuration documentation was completed.
- Verify that the CMDB and related configuration information is consistent with the physical state of all CIs, and vice versa.
- Verify the physical 'as-built' configuration of a CI conforms to its 'as-planned' configuration and its associated documents.
- Verify that correct and authorized versions of CIs exist, and that only such CIs exist, and are in use in the operational environment.
- Verify that change and release records have been properly authorized by Change Management and that implemented changes are as authorized.

Configuration audits should be considered at any of the following times:

- Following recovery from disasters and after a 'return to normal'
- At planned intervals (a minimum of quarterly during configuration management process implementation followed by annually thereafter)
- At random intervals at management's discretion
- In response to the detection of any unauthorized CIs

Baselines are the establishment of a current state within configuration management and are established at a specific point in time. Baselines are established just prior to a change being implemented so a known functioning state is documented to compare the change to and point from which an audit is conducted.

Metrics

The following metrics are the starting point and are expected to change and/or expand as Configuration Management is developed.

1. Assets identified as the cause of services failures
2. Exceptions reported during configuration audits
3. Changes that were not completed successfully or caused errors because of poor impact assessment, incorrect data in the CMS, or poor version control
4. These metrics will be developed as the process matures and the CMDB becomes populated.
5. Percentage of re-use and redistribution of under-utilized resources and assets tied to failure information
6. Reduction in the average time and cost of diagnosing and resolving incidents and problems by Type
7. Improved speed for incident management to identify faulty CIs and restore service

Training for Configuration Management Operations

Target Audiences

- Service techs
- Service Staff Managers

Syllabus

- Purpose of Configuration Management
- CMDB, CIs, and relationships
- Inputs and triggers
- Versioning and Naming Conventions
- Assets and Categories
- Hierarchies and Relationships
- Maintenance and Auditing
- Metrics

Delivery Options for training

- Video Conference
- Phone Conference
- Online Course

Training Sources

- Operations meeting notes

Chapter 6: Asset Management

Overview

Definition of Asset Management: Asset Management is the process responsible for tracking and reporting the value and ownership of financial assets throughout their lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process.

GOAL: The goal of Asset Management is to reduce IT expenditures, human resource overhead and risks inherent in owning and managing assets.

PURPOSE: is to integrate people, processes and technology to allow hardware, software, and associated licenses, contracts and agreements, and usage to be systematically tracked, evaluated and managed.

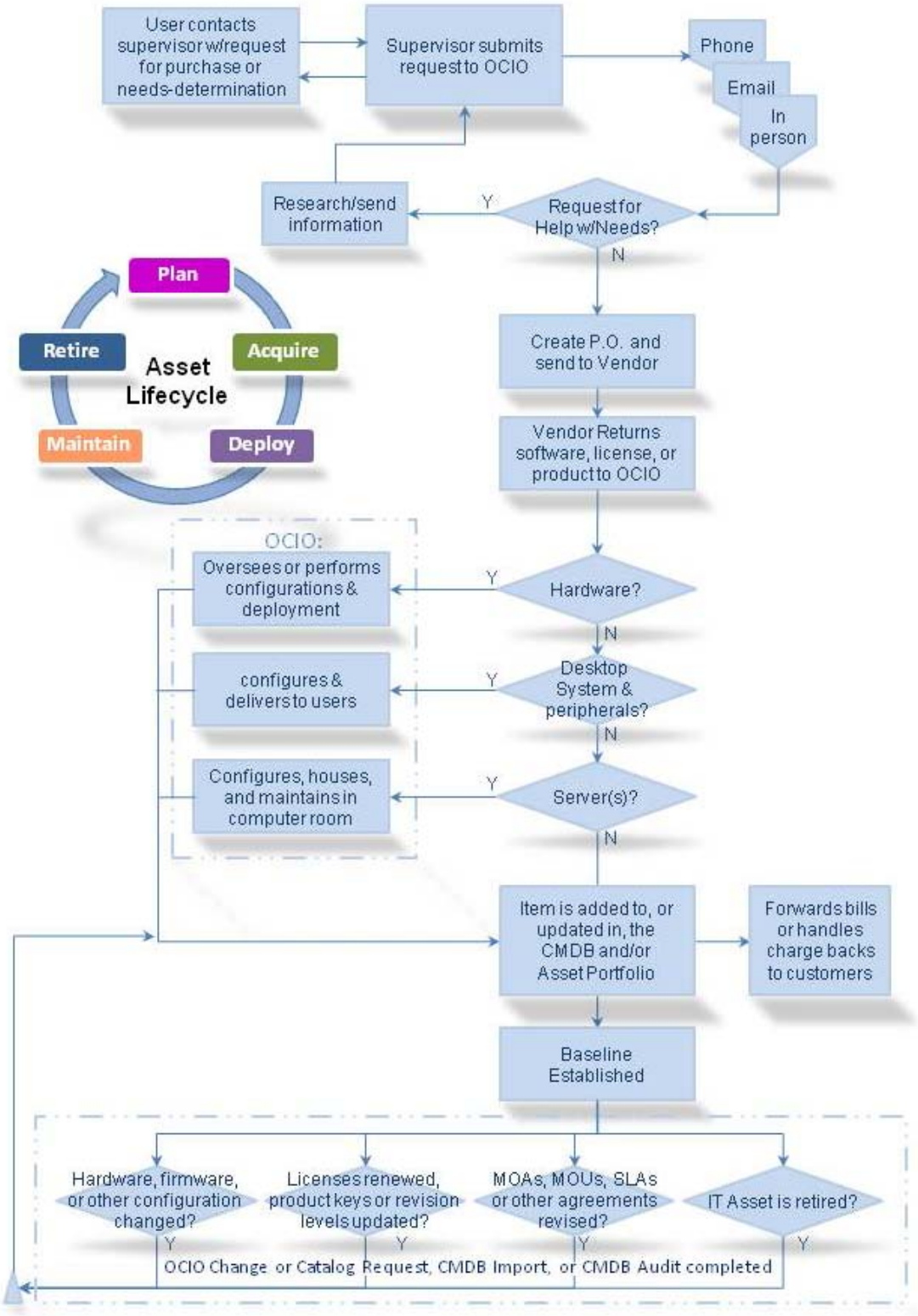
Asset Management – OCIO

The following information outlines the Asset Management program within the Office of the CIO for its assets and their relationship with the supported state agencies.

Assets managed by either the OCIO or supported agencies fall into 3 categories software, hardware and support/licensing agreements. All assets owned or supported by the OCIO will be recorded and tracked using the CMDB (Configuration Management Database) which is part of the Service Now system. The OCIO will conduct an annual audit of the CMDB coordinating with all agencies that have supported hardware and/or software. Responsibility for maintaining the asset information and its accuracy rests with the CI (configuration Item) owner with the OCIO.

Responsible Office/Agency	Software	Hardware	Support/Licensing Agreements
OCIO	• Approves all purchases • Maintains department software • Maintains Enterprise level software	• Approves Department purchases • Recommends purchases for supported agencies • Maintains servers • Maintains Department and supported agencies desktops	• Maintains department software • Owns Enterprise level agreements
Department of Admin	• OCIO submits the purchase request and the Division pays for required items	• OCIO submits the purchase request and the Division pays for required items	• OCIO submits the purchase request and the Division pays for required items
Supported Agencies	• Purchase approved items • Pay for Enterprise level software through charge backs	• OCIO may purchase or recommend required hardware	• Owns licensing requirements

Asset Management Procurement Process



Training for Asset Management Operations

Target Audiences

- OCIO Service techs
- Service Staff Managers
- Small Agency IT Supervisors
- Small Agency and OCIO Budget Staff

Syllabus

- Purpose of Asset Management
- CMDB and Asset relationships
- Order and Billing Process
- Asset Ownership
- Asset Maintenance and Renewal
- Assets Retirement

Delivery Options for training

- Video Conference
    - Phone Conference
- Online Course

Training Sources

- This manual

Chapter 7: Capacity Management

Overview

Definition of Capacity Management: Capacity Management is responsible for ensuring that the volume of IT services and their supporting IT infrastructure is able to deliver agreed service level targets in a cost effective and timely manner.

GOAL: The goal of Capacity Management is to provide sufficient information on capacity needs – taking into consideration all of the resources required to deliver promised services – to meet short, medium, and long term business requirements.

PURPOSE: Within the Service Delivery discipline of ITIL, Capacity Management helps organizations match their IT resources to business demands.

Stakeholders

The Office of the Chief Information Officer (OCIO) offers a wide variety of Information Technology services that would benefit from Capacity Management Planning. These services and their affected stakeholders include but are not limited to:

- **Communications** – Internet Services, Mass Email Distribution Group Services, Conferencing, Messaging
  - **Customers**
    - All Executive State Agencies
    - Elected Officials
    - Legislature
  - **Those Responsible for Providing Services**
    - OCIO – Enterprise Infrastructure (Network Services Group)
    - OCIO – Enterprise Infrastructure (Telephone Services Group)
    - OCIO – Enterprise Consolidated Services Group
  - **Systems Maintainers**
    - Internet Bandwidth Utilization
      - OCIO – Enterprise Infrastructure (Network Services Group)
    - Conferencing Service Utilization
      - OCIO – Enterprise Infrastructure (Telephone Services Group)
    - List Server
      - OCIO – Enterprise Consolidated Services Group

- **GIS** – Idaho spatial Data Infrastructure Management, Hosting Services
  - **Customers**
    - GIS Community (Federal, State, and Local government)
    - Citizens
  - **Those Responsible for Providing Services**

        - OCIO – Idaho Geospatial Office
    - **Systems Maintainers**
        - Data Storage Capacity
            - OCIO – Enterprise Infrastructure (Telephone Services Group)
        - Hosting (Server Capacity)
            - OCIO – Idaho Geospatial Office
            - OCIO – Enterprise Applications
            - OCIO – Enterprise IT Support Services

- **Hosting Services** – Database, Domain Name Services (DNS), File Transfer Services (DTP), Website Development, Website Hosting
    - **Customers**
        - All Executive State Agencies
        - Elected Officials
        - Legislature
        - Citizens
    - **Those Responsible for Providing Services**
        - OCIO – Enterprise Applications
    - **Systems Maintainers**
        - Database Storage Capacity
            - OCIO – Enterprise Applications
            - OCIO – Enterprise IT Support Services
        - DNS Server Utilization
            - OCIO – Enterprise Applications
        - FTP Server Utilization
            - OCIO – Enterprise Applications
        - Website Hosting (Web Servers utilization)
            - OCIO – Enterprise Applications

- **Networking** – Access to the state network
    - **Customers**
        - All Executive State Agencies
        - Elected Officials
        - Legislature
    - **Those Responsible for Providing Services**
        - OCIO – Enterprise Infrastructure (Network Services Group)
    - **Systems Maintainers**
        - Routing and Switching Equipment: memory utilization, port availability, feature set upgrade
            - OCIO – Enterprise Infrastructure (Network Services Group)
        - Circuit bandwidth utilization and capacity needs
            - OCIO – Enterprise Infrastructure (Network Services Group)

- **Security Services** – Firewall Management, Secure Remote Access, Spam and Virus Filtering
    - **Customers**
        - All Executive State Agencies

        - Elected Officials
        - Legislature
    - **Those Responsible for Providing Services**
        - OCIO – Enterprise Infrastructure (Network Services Group)
        - OCIO – Enterprise IT Security
    - **Systems Maintainers**
        - Firewall Hardware management
            - OCIO – Enterprise Infrastructure (Network Services Group)
        - VPN Client access connections and hardware management
            - OCIO – Enterprise Infrastructure (Network Services Group)
            - OCIO – Enterprise Infrastructure (Network Services Group)
        - IronMail Hardware management (spam/virus)
            - OCIO – Enterprise Infrastructure (Network Services Group)

- **Server management** – Backup Services, Server Administration
    - **Customers**
        - Agencies provided IT Support Services by the OCIO
    - **Those Responsible for Providing Services**
        - OCIO – Enterprise IT Support Services
        - OCIO – Enterprise Consolidated Services
    - **Systems Maintainers**
        - Backup systems hardware, data storage devices, tape media
            - OCIO – Enterprise IT Support Services
            - OCIO – Enterprise Consolidated Services
        - Server hardware and disk storage capacity
            - OCIO – Enterprise IT Support Services
            - OCIO – Enterprise Consolidated Services

Activities

Capacity Management Activities include identifying resources whose capacities have the potential to change, then identifying time frames, growth potentials, future needs of users (both current users and possible new users), and establishing metrics and other methods for recognizing planning and budgetary needs. Data gathering initially provides source information, then formatting the data consistently between like measurements, and finally, using the data to determine capacity thresholds through a regular review process are the main activities in the Capacity Management Process. The following breaks down these activities for OCIO-related services.

Data Gathering

For servers servicing the small agencies and networks supported by OCIO, data gathering should be done at specific intervals to create baselines and establish normal rates of change. Periodic reviews will be performed to monitor real-time loads, compare to normal rates, watch for developing issues, and monitor cyclical usage highs and lows.

Data will be provided in graphical format to better identify baselines, trends, and to identify actions to increase capacity. The agency or group performing the data gathering should

determine sampling intervals, monitoring software, and other methods and tools necessary to providing reliable capacity management information.

ICS Server Hardware Capacity

ICS hardware capacity will show the following information:

Element Measured	Percent of usage			Sampling Interval	Notes
	Green	Yellow	Yellow		
CPU	< 85%	86 – 95%	96%	Weekly	
Memory	86-95%		100%	Weekly	
Disk Capacity			>60%	Monthly	Show growth month by month against capacity with action prior to max capacity.
Number of Mailboxes				Monthly	Show growth month against current capacity with action prior to max capacity.

ICS Database Hardware Capacity

For ICS database servers the same monitoring will take place with attention and reporting on the following items:

Element Measured	Usage			Sampling Interval	Notes
	Green	Yellow	Yellow		
CPU	35-40%	40 – 64%	65%	Weekly	
Memory	< 75%	76 – 90%	90%	Weekly	
I/O Speed	1-2 R/W	3-4%	>5 R/W	Weekly	Measures Read/Writes Measuring number in queues.

Small Agencies

For servers servicing the small agencies supported by OCIO, monitoring will include:

Element Measured	Percent of usage			Sampling Interval	Notes
	Green	Yellow	Red		
CPU	65 – 85%	86 – 95%	96%	Weekly	
Memory	< 75%	76 – 90%	90%	Weekly	
I/O Speed	1–2	3–5	>5	Weekly	Measures around reads/writes; measuring #'s in queues
Disk Space				Monthly	

Networks

Network monitoring software which will do real-time monitoring and send alerts is best; however, consistent measurements compared with established baselines are essential. Taken at regular intervals, these should include:

Element Measured	Percent of usage			Sampling Interval	Notes
	Green	Yellow	Red		
CPU	65 – 85%	86 – 95%	96%	Weekly	
Memory	< 75%	76 – 90%	90%	Weekly	
Bandwidth	85 – 90%	90 – 95%	>95%	Weekly	Breakdown by segments
Reliability	Expressed as interface errors or discards			Weekly	
Latency/Response	Should be single digit miliseconds			Weekly	

Sample graphs for these monitored elements can be found in Appendix E: Capacity Management Data Gathering Graphical Samples

Capacity needs projections

Capacity Expansion Funding

Capacity expansion funding needs are addressed in three different approaches depending on the system(s). First, statewide systems which OCIO has primary responsibility for, except ICS, are funded through appropriations made from the legislature and are based on justified need. Second, systems which OCIO maintains for specific agencies are funded through direct funding from each of the agencies using the specific systems. Third, user fees are paid to OCIO, as in the case of ICS, which are intended to maintain the system so that it supports the needs of the users.

Determining future needs

The initial capacity measurements will establish baselines from which to start measuring capacity growth estimates. In lieu of tools which will measure growth patterns and perform capacity projections, the basic approach is to establish an initial baseline, establish the capacity thresholds (green, yellow, red) for each capacity being measured, and then establish measurement periods, e.g., weekly, monthly, etc. Measured growth rates are then applied to the growth chart to estimate when additional capacity is required.

The goal is to ensure capacity does not enter into the red threshold which can affect system performance and impact users. The time at which action needs to be taken to secure additional capacity depends on two things: when capacity is projected to become red, and; the steepness of the growth curve. Put into the context of the required lead times, these should be used to secure funding for the additional capacity.

Additional considerations for increased capacity needs, because of projects or new systems, should to be factored into the projections on a case by case basis.

Capacity Needs Funding

As a general rule, when projections identify capacity needs which will pass into the red threshold, planning for additional capacity should begin. If the additional capacity requires legislative funding, the timeline to secure the funding is long and dependant on the budgeting cycle. Budget inputs for capacity needs are to be submitted at least ten months before the next fiscal year begins. Because of the nature of the budgeting cycle, future needs identified in September of any given year may have to wait 18 months for funding. Funding for other capacity is dependent on individual agency budgets and planning requirements, as well, and will need to be coordinated with the respective agencies.

Program Reviews

Capacity Reviews

Quarterly review meetings by the OCIO Team Lead staff wil be used to:

- monitor, analyze, tune, and implement necessary changes in resource utilization;
- manage demand for computing resources, which requires an understanding of business priorities;
- ensure required service levels are being met;
- model to simulate infrastructure performance and understand future resource needs; and
- identify future capacity needs and take appropriate action to acquire, if needed.

Audits

Annual audit meetings by the OCIO Team Lead staff should be used to:

- measure current model performance against actual system performance to validate models.; and
- take appropriate action to adjust models, if needed.

Training

Training for OCIO Service Delivery disciplines is handled by team leads and staff at team levels through review and audit.

Chapter 8: Service Catalog

Overview

Definition of Service Catalog: A Service Catalog is a list of services that an organization provides to its employees, customers, or users.

GOAL: The goal of the Service Catalog is to elevate the perception of the IT organization to that of a Service Provider, move it closer to a service instead of a technical orientation, streamline access, approval, and delivery of services, and provide a base for formal Service Level Management.

PURPOSE: Within the Service Design discipline of ITIL, the Service Catalog is the starting point for efficiently documenting services, communicating services to users, and creating the foundation for negotiating the contracts and agreements that match service delivery to business needs

High-level Service Catalog Development Narrative

Development of the Service Catalog involves five basic steps:

1. Obtain management support, working with customers, users and technical staff to reflect the perceptions of all stakeholders.
2. Establish a team to examine and define the major services currently being provided by technical staff, and to define the needs and perceptions of the business service users.
3. Define the IT services. Document the services using the templates provided with the services in this chapter.
4. Review the catalog with IT staff and leads, and handle concerns and changes through engagement rather than edict.
5. Publish the Catalog on inter/intranet or other public sources and solicit responses.

Currently, OCIO services are published through this document and will be available online as time and resources allow.

OCIO Service Catalog

Products and Services

Communications
- Conferencing Services
- Internet Services
- Mass Email Distribution Group Services
- Messaging Services
- Voice and Mobile Services

Consulting
- PC Lease Management
- IT Purchasing

Geographic Information Systems (GIS) Services
- Idaho Spatial Data Infrastructure Management
- GIS Community Communications Administration
- GIS Consulting Advice, Recommendations, and Referrals
- GIS Hosting Map Applications and Feature Services

Helpdesk Services
- Helpdesk (Service Desk)

Hosting Services
- Database Services
- Domain Name Services (DNS) Requests
- File Transfer (FTP) Service
- Website Development
- Website Hosting

Networking
- Access to the state network

Security Services
- Firewall Management
- Cyber Security Incident Response
- Network Intrusion Detection
- Secure Remote Access
- Security Awareness Training
- Spam & Virus Filtering
- Vulnerability Assessments

Server and Desktop Management
- Backup Services
- Desktop Support
- Server Administration

Support Services
- Billing
- Consulting
- IT Support
- Project Management
-

State of Idaho Office of the CIO Service Catalog – Communications

Service Name	**Conferencing Services**
Service Description	Audio Conferencing - The audio conference bridge is provisioned to allow multiple simultaneous calls with up to 65 concurrent callers. All State agencies are welcome to become a bridge user and will be able to schedule their own audio conferences. In addition the State has a contract with AT&T for overflow calls and for callers that need advanced features such as call-recording or call transcription services.
Service Characteristics	• Multiple simultaneous calls with up to 65 concurrent callers • Conference Bridge services must be scheduled in advance at: http://conferencing.idaho.gov/ Choose Scheduling Application o Login and Password required to schedule services • Costs are based on number reserved ports • Video/Audio conferencing capability is available in the J.R. Williams East Conference Room • List of state agencies VTC installations can be located at: http://conferencing.idaho.gov/ Choose the VTC Directory option
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support services are available for this service **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time)
Clients of the Service	All State Agencies (executive and elected officials) can utilize this service
Business Processes Enabled by the Service	Allows agencies to conduct business and participate in meetings without the need to travel.
Customer Roles and Responsibilities	• Register to use the conference bridge • Use scheduling Application to schedule to use the conference bridge • Cancellations must be received 24-hours in advance prior to the scheduled conference or a penalty equivalent of the number of ports scheduled will be assessed and billed, • Contact the Service Desk to report problems. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	• Must have a user login and password • Online registration at http://conferencing.idaho.gov/register.htm • Online scheduling of bridge at: http://conferencing.idaho.gov:80/tms/Tandberg/TMS/UI/TandbergScheduler/
Cost Information	• Billing is based on the total number of ports reserved • $1.00 per each port (participant) • $0.05 per minute per person usage

State of Idaho Office of the CIO Service Catalog – Communications

Service Name	**Internet Service (Statewide Internet)**
Service Description	The Office of the CIO provides access to Internet services to all state agencies. The Enterprise Infrastructure team configures WAN and LAN components, firewall, and other network infrastructure, as appropriate, to ensure that agencies have the access needed to Internet services. In the current environment, this involves maintaining mutually redundant and supportive Internet points of presence on the Capitol Mall and in Meridian.
Service Characteristics	• Network and Internet connectivity • Designing and maintaining the state network infrastructure • Installing and maintaining network components (switches, routers, firewalls, and wireless) • Monitoring network traffic • Troubleshooting network failures and connectivity issues • Interfacing with external service providers • Planning for future capacity requirements or upgrades • Evaluating, recommending and purchasing of network equipment • Disaster planning and recovery
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 7:00PM – Mountain Time After hours including state holidays – Technicians on call **Note:** After hours support is for system emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted. **Service Level metric:** 99%
Clients of the Service	All State Agencies (Executive and Elected Officials)
Business Processes Enabled by the Service	This service supports access to the Internet for state agencies in a secure manner. Provides agencies the ability to establish a web presence in order to offer online services and information.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems with network or internet connectivity. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 1, sending email requests to helpdesk@cio.idaho.gov, or by accessing the Service Desk at http://idaho.service-now.com
Cost Information	At this time there is no cost for general Internet access as this is a generally funded service. Agencies can request Internet services specifically dedicated to their agency for a cost of $100 per Mb per month.

State of Idaho Office of the CIO Service Catalog – Communications

Service Name	**Mass Email Distribution Group Services (Statewide Listserv)**
Service Description	This service provides distribution lists for groups who need to send email to large populations. The advantage of this service is that the distribution list can contain email addresses of those who are on different state email system or on networks outside the state system.

Service Characteristics	• The ability to send an email to a single email address and reach large populations
	• Web Management tool for easy recipient administration and list configuration.
	• Example uses of this system are:
	  o ISEC list — used by the state IT managers to schedule meetings and discuss IT issues and problems
	  o WAN list — used by the state networking staff to communicate issues and problems, or to discuss general networking issues
	  o Cybersec list — used by agency IT security coordinators to discuss IT security topics, provide notification of newly discovered security vulnerabilities.

Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support is available for this service **Scheduled Maintenance Window:** Every Thursday 5:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	All State Agencies (executive and elected officials) can utilize this service
Business Processes Enabled by the Service	The ability to utilize email to reach a large customer base quickly and easily.
Customer Roles and Responsibilities	• Provide initial list of recipients • Define list characteristics • Maintenance of the list after creation by system administrators • Contact the Service Desk to report problems by any of the methods defined below. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	• For List Administration – must have a valid user ID and password, go to URL http://admws.idaho.gov/mailman/listinfo • To send an email to list recipients utilize any email client such as Outlook and address the message to the list's email address (listname@admws.idaho.gov). Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Communications

Service Name	**Messaging Services**
Service Description	The Office of the CIO currently provides email and directory services for executive state agencies as part of a statewide consolidated initiative. This service includes maintaining a statewide Microsoft Active Directory infrastructure as well as a centralized Exchange 2007 messaging system.
Service Characteristics	• E-Mail and Calendaring - Microsoft Outlook Client (Office 2003 or higher) • Mobile Device Synchronization and support (Windows Mobile and Blackberry) • Web Access Email – https://owa.ics.idaho.gov • Outlook Anywhere Email – Microsoft Outlook Client via RPC over HTTPS A valid user ID and password is required for all of the above options.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support is for system emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 5:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted. **Service Level metric:** 99.9% **Note:** Systems availability and uptime metric calculations exclude scheduled maintenance activities.
Clients of the Service	Executive Agencies transitioned to consolidating messaging and small agencies and commissions that receive their IT support from the OCIO.
Business Processes Enabled by the Service	This service supports electronic communication via email either local client or online with web access, via mobile devices, and scheduling via calendaring tools.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems by any of the methods defined below. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com
Cost Information	**If Agency has their own Exchange 2007 (or higher) Client Licensing with Software Assurance** 250Mb Mailbox - $1.50 per month 750Mb Mailbox - $12 per month 500Mb Mailbox - $8 per month 1Gb Mailbox - $16 per month **If ICS provides Exchange Client Licensing** 250Mb Mailbox - $2.42 per month 750Mb Mailbox - $15 per month 500Mb Mailbox - $10 per month 1Gb Mailbox - $20 per month Pricing information is also located at the following website: http://cio.idaho.gov/products_and_services/consolidated_messaging_project.htm

State of Idaho Office of the CIO Service Catalog – Communications

Service Name	**Voice and Mobile Services**
Service Description	**Voice Services** Coordinate the installation and configuration of telephone lines, systems, and services throughout the state for all agencies. Assist state agencies in identifying telephone equipment and service requirements, and then implement solutions to meet their requirements. **Mobile Services** Administer the contracts for cellular services and equipment. State agencies can obtain services, cellular phones, data devices, and airtime cards from AT&T Wireless (formerly Cingular), Sprint/Nextel, and Verizon Wireless. Analyze usage and recommend changes in calling and data plans. Review equipment and coverage needs, and make carrier and equipment recommendations. Test and review new cellular technology (such as PDAs). Negotiate and administer all statewide telephone services contracts.
Service Characteristics	• Statewide and local service • Statewide telephone equipment • Long distance • Toll-free Calling • Calling Cards • Language Translation • Cellular calling and mobile data • Payphones • Voice services billing • State telephone directory For specific details on each of the above services visit: http://cio.idaho.gov/products_and_services/voice_contracts.htm
Service Level Objectives	**Service Availability:** Monday through Friday 7:00AM through 5:00PM (Mountain Time) **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support is available for this service
Clients of the Service	All State Agencies (executive and elected officials) as well as other public entities such as cities, counties, and school districts can utilize this service
Business Processes Enabled by the Service	This service provides basic and advanced telecommunication functions that enable both internal and external communication.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems and request services by any of the methods defined below. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Services can be provisioned by calling (208) 332-1500 and choosing option 2, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com
Cost Information	•

State of Idaho Office of the CIO Service Catalog – Consulting

Service Name	**PC Lease Management Services Consulting**
Service Description	The Office of the CIO currently provides assistance to agencies that want to lease IT equipment; desktop computers, laptops, servers, and etc.
Service Characteristics	• Assist agencies in defining their IT requirements • Provide information and make recommendations on an agency-specific lease management solution • Work with the vendor to outline the agency's needs and obtain quotes • Submit equipment orders to the leasing company • The lease management solution is coordinated with the purchasing contracts negotiated through the Division of Purchasing. Statewide contracts can be found at: http://adm.idaho.gov/purchasing/stwidecntrcs.html.
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:30 AM to 5:00 PM (Mountain Time)
Clients of the Service	Small agencies and commissions that receive their IT support from the OCIO.
Business Processes Enabled by the Service	This service supports all agency IT operations to match the best solution to an agency's needs.
Customer Roles and Responsibilities	• Contact the OCIO Service Desk to request assistance • Provide agency specific needs so that the best solution can be reached • Adherence to all ICS, ITRMC, and appropriate state policies
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	The cost for this service is included in an agency's IT support costs.

State of Idaho Office of the CIO Service Catalog – Consulting

Service Name	**IT Purchasing Consulting**
Service Description	The Office of the CIO currently provides assistance to agencies that want to purchase IT equipment; desktop computers, laptops, servers, and etc. Our goal is to ensure that the agency gets the products that they need at the best possible price.
Service Characteristics	• Assist agencies in defining their IT requirements • Provide information and make recommendations on available purchasing options • Work with the vendor to outline the agency's needs and obtain quotes • Submit equipment orders to the vendor • The IT purchasing solution is coordinated with the purchasing contracts negotiated through the Division of Purchasing. Statewide contracts can be found at http://adm.idaho.gov/purchasing/stwidecntrcs.html.
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:30 AM to 5:00 PM (Mountain Time)
Clients of the Service	Small agencies and commissions that receive their IT support from the OCIO.
Business Processes Enabled by the Service	This service supports all agency IT operations to match the best solution to an agency's needs.
Customer Roles and Responsibilities	• Contact the OCIO Service Desk to request assistance • Provide agency specific needs so that the best solution can be reached • Adherence to all ICS, ITRMC, and appropriate state policies
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	The cost for this service is included in an agency's IT support costs.

State of Idaho Office of the CIO Service Catalog – GIS

Service Name	**Idaho Spatial Data Infrastructure Management**
Service Description	The Idaho Geospatial Office facilitates and manages The Idaho Map.
Service Characteristics	The Idaho Map is a collection of technical and human resources specifically organized to develop, maintain, and provide access to digital base maps in a collaborative, multi-organization environment. • Framework development (base geospatial data) and stewardship • License agreements and data sharing networks • Enterprise service development and deployment • Data sharing initiatives • Distributed capabilities and services **Enterprise services include:** • Planning multi-agency architecture • Implementing a robust infrastructure to support enterprise services • Facilitating interdepartmental technical solutions • Hosting core applications (like a geocoding engine) and web services **GIS Data Integration and Enterprise Deployment:** • Blending independently developed databases forming a single authoritative source • Plan, design, and implement robust backbone solutions to serve many business purposes and agencies
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:30 AM to 5:00 PM (Mountain Time)
Clients of the Service	• Idaho's educational institutions • Idaho's government agencies • Idaho's business and industry • Idaho's private citizens • Tribal governments • Associations and nongovernmental organizations • Elected officials
Business Processes Enabled by the Service	• Help decision makers visualize and understand complex situations, patterns and relationships; identify and compare the merits of alternative scenarios; more accurately predict outcomes; engage stakeholders to build consensus; and evaluate the effectiveness of actions taken. • Provide accurate and reliable base data to fuel applications for decisions about the security, prosperity, health and safety of our citizens and organizations.
Customer Roles and Responsibilities	• Contact the OCIO Service Desk to request assistance • Provide agency-specific needs so that the best solution can be reached • Adherence to all ICS, ITRMC, and appropriate state policies
How to Access the Service	Services can be accessed by calling (208) 332-1879, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – GIS

Service Name	**GIS Community Communications Administration**
Service Description	The Idaho Geospatial Office can add users to the GeoTech Listserv and provide access to other communications approaches.
Service Characteristics	Geo Tech Listserv: • Can be accessed at http://admws.idaho.gov/mailman/listinfo/geotech. Login and password are required. • Is an open forum and not an official technical support resource. • It is designed to stimulate discussion and collaboration on geospatial technologies, data, stewardship, and related topics. • We invite you to share announcements and information, discuss issues and facilitate collaborative efforts relevant to delivering geospatial technology solutions to decision makers. • To post a message to geotech, send an email to: geotech@admws.idaho.gov • Geo Tech Listserv is not a moderated list. Anything sent to geotech@admws.idaho.gov will be broadcast (unedited) to subscribers.
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:30 AM to 5:00 PM (Mountain Time)
Clients of the Service	• Idaho's educational institutions • Idaho's government agencies • Idaho's business and industry • Idaho's private citizens
Business Processes Enabled by the Service	This service facilitates communications and keeps everyone in the GIS community abreast of opportunities and developments.
Customer Roles and Responsibilities	• Contact the OCIO Service Desk to request assistance • Provide agency-specific needs so that the best solution can be reached • Adherence to all ICS, ITRMC, and appropriate state policies
How to Access the Service	Services can be accessed by calling (208) 332-1879, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – GIS

Service Name	**GIS Consulting Advice, Recommendations, and Referrals**
Service Description	The Idaho Geospatial Office provides consulting advice and recommendations for Geographic Information Systems. We facilitate the use, development, access, sharing, and management of geospatial data and assist with communicating the value of geospatial information to citizens and decision-makers in the state of Idaho. If we don't have the answers or are unable to provide sufficient help, we connect inquirers with the best resources available to address their specific issue or question.
Service Characteristics	Geographic Information Systems (GIS) is a collection of technical and human resources specifically designed for geospatial information and the part of information technology that focuses on capturing, managing, analyzing, and displaying features and their attributes to support decision making. • Geospatial data development and stewardship • System, software, and data purchases • Enterprise service development and deployment • Data sharing initiatives **Enterprise services include:** • Planning multi-agency architecture • Implementing a robust infrastructure to support enterprise services • Facilitating interdepartmental technical solutions • Hosting core applications (like a geocoding engine) **GIS Data Integration and Enterprise Deployment:** • Blending independently developed databases • Plan, design, and implement backbone solutions to serve many business purposes and agencies
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:30 AM to 5:00 PM (Mountain Time)
Clients of the Service	All State Agencies (executive and elected officials) can utilize this service
Business Processes Enabled by the Service	• Help decision makers visualize and understand complex situations, patterns and relationships; identify and compare the merits of alternative scenarios; more accurately predict outcomes; engage stakeholders to build consensus; and evaluate the effectiveness of actions taken • Provide accurate and reliable base data to fuel applications for decisions about the security, prosperity, health and safety of our citizens and organizations • Spatially enable tabular databases
Customer Roles and Responsibilities	• Contact the OCIO Service Desk to request assistance • Provide agency specific needs so that the best solution can be reached • Adherence to all ICS, ITRMC, and appropriate state policies
How to Access the Service	Services can be accessed by calling (208) 332-1879, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – GIS

Service Name	**GIS Hosting Map Applications and Feature Services**
Service Description	The Idaho Geospatial Office can host map applications and web services.
Service Characteristics	• Host map applications and web services on shared servers. • Share data, resources, technologies, and expertise to meet the increasing demands for Idaho's geospatial information. • Provide leadership and expertise in the storage, support, archiving, and distribution of Idaho's digital geospatial data. • Provide a framework for cost-effective collaboration, the exchange of technological expertise and ideas, and the sharing of digital spatial and statistical data.
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:30 AM to 5:00 PM (Mountain Time)
Clients of the Service	All State Agencies (executive and elected officials) can utilize this service
Business Processes Enabled by the Service	Assist agencies to meet geospatial capacity needs with a shared solution.
Customer Roles and Responsibilities	• Contact the OCIO Service Desk to request assistance • Provide agency-specific needs so that the best solution can be reached • Adherence to all ICS, ITRMC, and appropriate state policies
How to Access the Service	Services can be accessed by calling (208) 332-1879, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Helpdesk Services

Service Name	**Help Desk (Service Desk)**
Service Description	To act as a single point of contact between the OCIO Services clients and OCIO Services areas. Activities include: • Receiving and recording of all inquiries from all OCIO Services clients. Capturing all relevant information from the client on the first contact. • Providing an initial assessment and attempting first call resolution, if appropriate. • Upon completion, promptly updating and closing incidents with full descriptions of incident resolution and/or service delivery • Determining urgency and impact levels (prioritization) for an incident if it cannot be resolved during initial contact to the Service Desk. • Dispatching unresolved incidents to second- and/or third-level support. • Routing service requests (requests for new work) to appropriate OCIO Service area. • Facilitating communication to clients regarding IT Services advisories (e.g. scheduled maintenance and other notices). • Escalation of Break / Fix requests according to service levels.
Service Characteristics	**Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) For the Department of Administration and small agencies without their own 1st level support, the Help Desk provides 1st level support, for other agencies, the Help Desk provides 2nd level support activities.
Service Level Objectives	Priority is set by determining how urgent the incident is, and what its immediate impact is. Urgency is synonymous with how heavily work is impaired, while impact is synonymous with the number of people whose work is affected. Urgency and Impact can be set by selecting from drop down lists where the choices are assigned values, and priority can be calculated. Resolution times are filled in based on MOAs developed with each agency. Priority may be changed upon escalation. * Note – Troubleshooting and resolution will be coordinated by the Service Desk and dispatched to the appropriate IT Services group.
Clients of the Service	Clients directly supported by the OCIO Desktop support and all other state agencies using state offered services.
Business Processes Enabled by the Service	This service supports the process for managing technology-related inquiries for all OCIO Services clients. This service is critical as it: • Provides a single point of contact for clients • Delivers responsive support to state government business services • Supports changes across business, technology and process boundaries
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services are accessed by calling (208) 332-1500, email requests sent to Helpdesk@CIO.Idaho.gov or accessing the Service Desk at www.idaho.service-now.com
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Hosting Services

Service Name	**Database Hosting**
Service Description	The Office of the CIO provides database servers on which state agencies can store public and agency confidential data, and staff to manage the servers, data security, and support for the data systems.
Service Characteristics	• Hosting for MSSQL2005 databases. • Publicly accessible database servers for hosting databases outside the state's firewall. • Protected copies of publicly accessible data and true copies of secure data on database servers behind state firewalls. • Backups of data to disk and tape maintained on- and off-site for quick restore or disaster recovery, as required. • Staff to configure, update, upgrade, and maintain servers. • Optimizations, indexing, and reporting run on databases reqularly. • Security maintained for each agency on shared servers. • Consulting on database schema, security, and all development activities. • Assistance when hiring consultants or contractors for database-related projects.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 8:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support is for system emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 5:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted. **Service Level metric:** 99%
Clients of the Service	All State Agencies
Business Processes Enabled by the Service	This service supports data used for state agencies' web and non-web applications in a secure manner. Provisions small agencies without resources to acquire database servers, and larger agencies desiring additional data services accessible by the public.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems with database connectivity, or data accessibility issues, giving exact error messages. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 4, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com/
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Hosting Services

Service Name	**Domain Name Services (DNS) Service**
Service Description	**Domain Name Services and Domain Management** The Office of the CIO provides Domain Name System (DNS) services to State of Idaho agencies as well as city, county, and local government. These DNS services allow for complete domain management, including domain registration and conflict mitigation, for two State government enterprise domains (IDAHO.GOV and STATE.ID.US) and one enterprise domain (ID.GOV) that is specifically reserved for city, county, and other local government agencies. **DNS Hosting** The Office of the CIO also provides DNS resource records hosting and propagation to any state agency for any domain or domains they have in use. This includes .com, .net, .org, and .us domains.
Service Characteristics	The State's DNS service is comprised of four different DNS servers in two physically different locations, providing redundancy, security, and high availability to the State's critical electronic identity. **Enterprise Hosted Domains** • IDAHO.GOV • ID.GOV • STATE.ID.US
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support is for system emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted. **Service Level metric:** 99.99%
Clients of the Service	All State Agencies (executive and elected officials) as well as other public entities such as cities, counties, and local government can utilize this service.
Business Processes Enabled by the Service	Provides agencies the domain recognition to send and receive email messages and the ability to establish a web presence in order to offer online services and information.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems by: o calling (208) 332-1500 and choose option 4; o Sending email requests sent to helpdesk@cio.idaho.gov ; o accessing the Service Desk at http://idaho.service-now.com • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.

How to Access the Service	**State Agencies:**
	• Request a third-level IDAHO.GOV domain name at:
	  o http://idaweb.state.id.us/dnsreg/
	• Manage your DNS records for both the IDAHO.GOV and STATE.ID.US domains at:
	  o http://idaweb.state.id.us/dnsreg/
	Public Agencies (non-state government entities such as counties and cities):
	  o Request a third-level ID.GOV domain name (the page includes a registration form, as well as the rules and requirements)at:
	  o http://cio.idaho.gov/products_and_services/domain_name_services/ID.GOV_DNS_registration/

Cost Information	Currently there are no costs associated for the IDAHO.GOV, ID.GOV, and STATE.ID.US domain hosting service. Agencies are responsible for any 3rd party domain registration costs related to their .com, .net, .org, and .us domains being hosted.

State of Idaho Office of the CIO Service Catalog – Hosting Services

Service Name	**File Transfer (FTP) Service**
Service Description	The Office of the CIO provides FTP connectivity between state agencies and their outside vendors/partners for secure, quick, and easy transfers of large-volume or material-sensitive files for which email is not appropriate or realistic.
Service Characteristics	• This service currently operates on two dedicated FTP servers • Each agency will be provided their own individual directory structure so that access is limited to the particular agency and their business partners. • Anonymous logins are not allowed • Logins and passwords are required for access
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hour support services are available **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	All State Agencies (executive and elected officials) as well as their selected business partners.
Business Processes Enabled by the Service	Provides state agencies the ability to share large amounts of information with their business partners electronically in a secure manner.
Customer Roles and Responsibilities	• Provide list of business partner recipients; • Proactively manage/monitor their directory structure on the FTP servers; • Contact the Service Desk to report problems; • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	• Requests for Services or to report an issue can be accessed by calling (208) 332-1500 and choosing option 4, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at: http://idaho.service-now.com • Logins and passwords are required to use the FTP service
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Hosting Services

Service Name	**Website Development**
Service Description	Access Idaho the state's web portal provider offers website and webapp development and creation services. The Office of the CIO offers limited website design services such as consulting and assisting with design related issues. The Office of the CIO also provides a testing and development environment that is available for all state agencies to use.
Service Characteristics	**Website Design** • Start-to-finish website and portal design services. • Provide consulting services for website design and development to include design guidelines • Business analysis and user requirements definition • Information architecture and interaction design • Visual and interface design • Website maintenance • Assist agencies with design-related issues **Web Application Development Services** • Start-to-finish webapp development and creation services are obtainable through Access Idaho **Intranet Web-based Business Application Development Services** • Start-to-finish intranet-specific, web-based business application development and creation services are obtainable through Access Idaho **Website and Webapp Development and Testing Area** • A full-featured testing and development area is available to all state agencies for website and webapp testing and development. • The Windows IIS server is configured to use JAVA, JavaScript, Cold Fusion MX 7, .NET Framework 1.1 and 2.0, and FrontPage 2002 server extensions. • There is no PERL or FrontPage 2000 support currently configured on the test/development server. • The test/development server is available only to state-network-connected users. • Personnel connecting from outside the state network must create a Virtual Private Network (VPN) connection to see webpages and webapps on this server.
Service Level Objectives	**Service Availability:** Enterprise state Internet and Intranet web servers 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours support is available only for the state's enterprise Internet and Intranet servers. NO after hours support is available for design and development services. **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user

	community impacted.
Clients of the Service	All State Agencies (Executive and Elected Officials)
Business Processes Enabled by the Service	Provides agencies the ability to establish a web presence in order to offer online services and information.
Customer Roles and Responsibilities	• Contact the CIO Service Desk to report problems. • Contact Access Idaho for development services. • Submit requests for hosting services to the CIO Service Desk. • Visit the Web Application Development website for information related to the development processes and what the agency can expect at: http://idaho.gov/ai/working_with/ • Fill out an Access Idaho "Letter of Engagement" also located at the above website • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	**Office of the CIO** Services can be accessed by calling (208) 332-1500 and choosing option 4, sending email requests to helpdesk@cio.idaho.gov , or by accessing the Service Desk at http://idaho.service-now.com **Access Idaho (AI)** Services can be accessed by visiting the Web Application Development website at: http://idaho.gov/ai/working_with/ Call the AI office at: (208) 332-0102, contact Jeff Walker (General Manager) at Jeff@accessidaho.org, or contact Rich Steckler (Director of Marketing) at Rich@accessidaho.org
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Hosting Services

Service Name	**Website Hosting Service**
Service Description	The Office of the CIO provides central website hosting services for state agencies.
Service Characteristics	**Public Website Hosting Services** • Website hosting services are available for public websites for any state agency on Windows/IIS and Linux/Apache web servers • The Windows servers are configured to use PERL, JAVA, JavaScript, ColdFusion MX7, .NET Framework 1.1 and 2.0, and Microsoft FrontPage 2000 and 2002 Server Extensions. • The Linux servers are configured to use PHP, PERL, JAVA, JavaScript, and ColdFusion MX7. **Intranet Website Hosting Services** • Website hosting services are available for intranet websites for any state agency on a Windows IIS web server with JAVA, JavaScript, Cold Fusion MX 7, .NET Framework 1.1 and 2.0, and FrontPage 2000 and 2002 server extensions. PERL support is not currently configured. • The intranet server is available only to state-network-connected users. • Personnel connecting from outside the state network must create a Virtual Private Network (VPN) connection to see webpages and webapps on this server **Website Statistics Reporting Services** Weekly, monthly, or quarterly WebTrends website statistics reports for any hosted website. **Website Search Indexing Services** Full-text indexing for search, indexing can run daily, weekly, monthly, or quarterly.
Service Level Objectives	**Service Availability:** Enterprise state Internet and Intranet web servers 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours support is available only for the state's enterprise Internet and Intranet servers. NO after hours support is available for website hosting services. **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	All State Agencies (Executive and Elected Officials)
Business Processes Enabled by the Service	Provides agencies the ability to establish a web presence in order to offer online services and information.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Submit requests for hosting services to the CIO Service Desk. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 4, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Networking

Service Name	**Access to the State Network**
Service Description	Operation and administration of the Idaho State Network Infrastructure which includes: • The Capitol Mall Fiber Optic Network of Idaho CMFONI. A fiber optic network interconnecting 14 buildings on and around the Capital Mall; • WAN Services (including Idanet) – 200+ routers and switches that form the state's wide-area network; and • Coming soon a Metropolitan Area network to include the Boise Metro Area, Nampa, and Caldwell. • The Idaho Education Network (IEN) is outside the scope of the state network. Information related to IEN is located at: www.ien.idaho.gov
Service Characteristics	• Designing and maintaining all logical network structures • Installing and maintaining all network components (switches, routers, firewalls, and wireless) • Installing and maintaining network management software • Monitoring network traffic, events and failures using Network Management Software • Performing tuning on all network segments • Troubleshooting network failures and connectivity problems • Interfacing with external service providers and external contractors • Ensuring network security through the use of filters, access lists and firewall configuration • Planning for future capacity requirements or upgrades • Evaluating, recommending and purchasing of network equipment • Researching technological developments for networking • Disaster planning and recovery • Coordinating the planning and wiring of LANs
Service Level Objectives	**Service Availability:** state network infrastructure 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call NOTE: After hours support does not include an agency's Local Area Network (LAN) or their local connectivity (last mile) to the state network infrastructure. Support for these services is available during normal business hours. **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted. **Service Level metric:** 99%
Clients of the Service	All State Agencies (Executive and Elected Officials)

Business Processes Enabled by the Service	This service supports the network infrastructure for the state providing connectivity to state services and supported systems including Data, VoIP, Video, Audio, and connectivity to the Internet.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems with network or internet connectivity. • For those agencies not directly supported by the OCIO have their IT technical staff troubleshoot the issue first before contacting the service desk to verify it is not an agency related issue. Once determining the issue is not agency related the agency's technical staff must be available to assist in troubleshooting the issue with OCIO staff. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	To report issues or provision for services call (208) 332-1500 and choose option 1, send email requests to helpdesk@cio.idaho.gov , or access the Service Desk at http://idaho.service-now.com Information related to Idaho Education Network can be located at: www.ien.idaho.gov
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Firewall Management**
Service Description	Manage the state's primary firewall systems that provide protection between the state's network and the Internet. Provide management of agency-level firewalls (installed internally on the state's network) for those agencies that do not have the internal staff to support these systems.
Service Characteristics	• Monitor, maintain, and manage firewall hardware and software. • Update firewall configurations to allow access for new state applications or websites. • Modify the firewall policies based on changing threats. • Configure firewall rules for Network Address Translation (NAT), network access, and Virtual Private Network (VPN) requirement
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 6:30AM to 7:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support is for system affecting emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	State Agencies Using Internet Services
Business Processes Enabled by the Service	Initial Defense of the State Network Infrastructure
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 1, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Cyber Security Incident Response**
Service Description	A cyber security incident is considered to be any adverse event that threatens the confidentiality, integrity, or accessibility of an agency's information resources
Service Characteristics	This team will assist agencies in incident analysis and response activities. Such as: • attempts (either failed or successful) to gain unauthorized access to a system or its data • disruption or denial of service • unauthorized use of a system for the transmission, processing, or storage of data • changes to system hardware, firmware, or software without the agency's knowledge, instruction, or consent • attempts to cause failures in critical infrastructure services or loss of critical supervisory control and data acquisition (SCADA) systems • attempts to cause failures that might cause loss of life or significant impact on the health or economic security of the agency and/or state • probing of any nature that an agency or other authorized entity has not approved in advance for system security testing purposes • website defacements • virus or other malicious-ware outbreaks
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support are for system affecting emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 5:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	State Agencies Connected to the State Network
Business Processes Enabled by the Service	• Initial Defense of the State Network Infrastructure • Protection of State Network Infrastructure
Customer Roles and Responsibilities	• Contact the Service Desk to request assistance. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 5, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Network Intrusion Detection**
Service Description	The primary focus of the intrusion-detection system (IDS) is identifying and preventing threats from the Internet
Service Characteristics	• monitoring and analyzing user and system activities for specified systems • analyzing system configurations and vulnerabilities • assessing system and file integrity • monitoring for patterns typical of attacks • analyzing abnormal activity patterns • tracking user policy violations
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support is for system affecting emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	State Agencies Connected to the State network
Business Processes Enabled by the Service	• Initial Defense of the State Network Infrastructure • Protection of State Network Infrastructure
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 5, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Secure Remote Access**
Service Description	The State of Idaho virtual private network (VPN) service provides state employees with a way to connect securely to the state's network.
Service Characteristics	• Establish and document VPN configurations. • Configure, provision, support, and troubleshoot individual accounts. • Develop and provide training to all VPN users.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 10:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support are for system affecting emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 7:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	State Agencies Connected to the State network
Business Processes Enabled by the Service	• Initial Defense of the State Network Infrastructure • Protection of State Network Infrastructure • Remote User Connectivity
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 5, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Security Awareness**
Service Description	In order for these employees to trust the confidentiality, integrity, and accuracy of the information with which they work, all employees need to be a part of the security solution and must be aware of what the security environment is.
Service Characteristics	• Education about: Hackers, Scammers, or purveyors of malicious software. • Preparation of security awareness materials • Provision of a custom training plan based on agency needs.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time)
Clients of the Service	State Agencies Connected to the State network
Business Processes Enabled by the Service	• End user Security Awareness • Educated workforce • Risk Mitigation and threats to infrastructure through awareness.
Customer Roles and Responsibilities	• Contact the Service Desk to request training. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 5, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Spam & Virus Filtering**
Service Description	All users on the state network have their incoming email processed by an email scanning and virus solution for to protect the network from malicious software and to drastically reduce spam and scam email from reaching state employees.
Service Characteristics	• Dramatically reduce the amount of unwanted (SPAM) emails delivered to state email boxes. • Quarantine capabilities allow the agency to make the final decision. • Training for agencies on the products and techniques used in filtering. • Whit listing and Blacklisting services.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) After hours including state holidays – Technicians on call **Note:** After hours support is for system emergencies only and is not intended for end-user helpdesk support **Scheduled Maintenance Window:** Every Thursday 7:00PM – 10:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	State Agencies Connected to the State Network
Business Processes Enabled by the Service	• Initial Defense of the State Network Infrastructure • Protection of State Network Infrastructure • Reduction of unwanted electronic correspondence.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 5, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Security Services

Service Name	**Vulnerability Assessments**
Service Description	By using vulnerability scanning, we remotely scan the network to identify known vulnerabilities and security weaknesses. Networks are easily analyzed from the perspective of the outside attacker, and with that information, we can improve the security of the systems that are scanned and evaluated.
Service Characteristics	• Limited Scanning of Servers and Workstations • Website Vulnerability Scanning • Can provide tools to an agency to allow them to specifically scan a suspect system.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 6:30AM to 7:00PM (Mountain Time)
Clients of the Service	State Agencies connected to the State Network.
Business Processes Enabled by the Service	Initial Defense of the State Network Infrastructure
Customer Roles and Responsibilities	• Contact the Service Desk to request assistance. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 5, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Server and Desktop Management

Service Name	**Backup Services**
Service Description	The Office of the CIO provides data backup solutions and backup consulting for state agencies in the event of a hardware failure or disaster.
Service Characteristics	• installing and configuring backup software • configuring for full, incremental, and differential backups • providing backup solutions and support for tape, CD, DVD, direct-attached storage (DAS), network-attached storage (NAS), and/or storage-area network (SAN) • rotating the media using the grandfather-father-son rotation scheme (or a scheme tailored to the agency's needs) • coordinating offsite storage, pickup, and delivery of media through the State Record Center • restoring and testing the restoration • monitoring and notifying customers of successful or failed backups
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) **Scheduled Maintenance Window:** Every Thursday 5:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	CIO Supported Agencies
Business Processes Enabled by the Service	Disaster Recovery
Customer Roles and Responsibilities	• Contact the Service Desk to request services • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	The cost for this service is included in an agency's IT support costs.

State of Idaho Office of the CIO Service Catalog – Server and Desktop Management

Service Name	**Desktop Services for OCIO Supported agencies**
Service Description	The Office of the CIO offers "Level 1" support to users by assessing general problems with their computer and network-connected peripheral equipment.
Service Characteristics	• assisting users to troubleshoot basic network, software, and printing problems • installing software, patches, and updates on desktop and laptop equipment • troubleshooting hardware issues and replacing hardware on both desktop and laptop equipment • installing, configuring, and testing desktop and laptop equipment, peripheral equipment, and software • working with vendor support contacts to resolve technical problems with desktop and laptop equipment and software • ensuring that desktop and laptop equipment interconnect seamlessly with diverse systems including associated validation systems, file servers, email servers, computer conferencing systems, application servers, and administrative systems • working with procurement staff to purchase hardware and software • ordering computer supplies
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) **Note:** After hours support is for system affecting emergencies only and is not intended for end-user helpdesk support
Clients of the Service	CIO supported desktop users
Business Processes Enabled by the Service	This service supports all agency IT operations to match the best solution to an agency's needs.
Customer Roles and Responsibilities	• Contact the Service Desk to request service or report problems. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	The cost for this service is included in an agency's IT support costs.

State of Idaho Office of the CIO Service Catalog – Server and Desktop Management

Service Name	**Server Administration for CIO Supported Agencies**
Service Description	Provide all aspects of server installation, configuration, and technical support of Servers.
Service Characteristics	• Server setup, patching, troubleshooting, and updating • Monitor servers to detect conditions such as overheating, processor failure, and disk failure, and to quickly alert an operator, take remedial action, or do both to maintain server performance. • Support servers that provide core services such as file, application, and printing services to the agencies. • Provide web servers to host agencies' websites • Provide a SQL server to host public-facing data used in agency online applications.
Service Level Objectives	**Service Availability:** All systems 24x7x365 **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) **Scheduled Maintenance Window:** Every Thursday 5:00PM – 7:00PM (Mountain Time) Prior to the maintenance window usage Email notices will be sent regarding the nature of the maintenance to be performed, expected down times, and user community impacted.
Clients of the Service	CIO Supported Agencies
Business Processes Enabled by the Service	This service supports all agency IT operations to match the best solution to an agency's needs.
Customer Roles and Responsibilities	• Contact the Service Desk to report request services. • Adherence to all ICS, ITRMC, and appropriate state policies.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com.
Cost Information	The cost for this service is included in an agency's IT support costs.

State of Idaho Office of the CIO Service Catalog – Support Services

Service Name	**Billing Services**
Service Description	The Office of the CIO provides comprehensive billing services as well as integrating and managing existing and new technology-related billing processes.

Service Characteristics	Billing services include:
	• Reviewing voice and technology-related invoices on behalf of state agencies for errors
	• Billing agencies for shared services to include:
	  o Internet service
	  o Idanet communications changes
	  o Capitol Mall Fiber Optic Network of Idaho (CMFONI) access
	  o Agency IT support
	• Billing agencies for their voice, conferencing, and data circuits Services

Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support for these services
Clients of the Service	All State Agencies (Executive and Elected Officials)
Business Processes Enabled by the Service	Central Services billings can be included in the Statewide Cost Allocation Plan (SWCAP). Shared services lower the overall costs of doing business by aggregating the buying power of the state. Identifying vendor billing errors can save the agency and the state money.
Customer Roles and Responsibilities	• Contact the Service Desk to report problems. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 2 for voice, conferencing, and data circuit related billings; choose option 3 for shared services billings. Send email requests to helpdesk@cio.idaho.gov or access the Service Desk at http://idaho.service-now.com
Cost Information	• Currently there are no additional costs for billing services related to the shared services indicated above. • There is an administrative fee for processing voice, conferencing, and data circuit billings.

State of Idaho Office of the CIO Service Catalog – Support Services

Service Name	**Consulting Services**
Service Description	The Office of the CIO offers consulting services to State agencies, users, and IT staff needing assistance in identifying and providing solutions to IT-related business needs, issues, or problems.
Service Characteristics	Consulting services typically include but are not limited to: • guidance on future technologies; • Assistance in determining the appropriate hardware and software needs and specifications; • Obtaining hardware and software cost information; • Providing guidance when determining the need for custom applications, off the shelf products, or project development; • Assistance with vendor related discussions; • Providing technical guidance on custom application projects; • Confirming or reviewing external or internal IT solutions • Reviewing and suggesting backup solutions • Assisting agency IT staff in troubleshooting problems • Assistance with developing or reviewing Disaster Recovery and/or Business Continuity solutions
Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support for these services
Clients of the Service	Small agencies, boards, and commissions that do not have their own IT support personnel. Any state agency needing assistance with those areas of IT where they lack appropriate technical expertise (such as in voice services, and wide area networking).
Business Processes Enabled by the Service	This service supports the process for: • Determining appropriate needs of an IT solution • Obtaining best practices business solutions • Supporting strategic goals
Customer Roles and Responsibilities	• Contact the Service Desk or any of the OCIO services managers to request consulting services. • Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.
How to Access the Service	Consulting Services can be accessed by: • Calling (208) 332-1500 and choosing from the options available the service area that might be best suited for the specific need. • Send email requests to helpdesk@cio.idaho.gov • Access the Service Desk at https://www.service-now.com/idaho/navpage.do • Calling an OCIO Leadership Team Manager o Leadership Team Manager contact information can be found at: http://cio.idaho.gov/customer_service/contact_list.htm
Cost Information	There are currently no costs associated with this service.

State of Idaho Office of the CIO Service Catalog – Support Services

Service Name	**IT Support (small agency)**
Service Description	The Office of the CIO offers general IT support services to any small agency, board, or commission needing IT support services who does not have their own IT support staff.

Service Characteristics	• Desktop Hardware Support – Hardware is defined as desktops, laptops, PDAs, printers, and scanners (Macintosh excluded).
	• Support is not offered on any equipment personally belonging to employees.
	• Desktop Software Support – supported software includes the most current version and its immediately preceding version of the following software:
	  o Microsoft Office Productivity Suite
	  o Microsoft Applications Software
	  o Microsoft Outlook client
	  o McAfee Antivirus software
	  o Adobe Acrobat, and Reader
	  o Microsoft Desktop Operating System (Linux is excluded)
	  o Employee Appraiser
	• Server Support
	• Networking and wireless network support
	• Virtual Private Network (VPN) support
	• Data Backup and recovery
	• Database Administration
	• Web Server Services
	• Consulting services
	• Preparation of Bid specifications
	• A copy of the Support Services Service Agreement detailing the above services can be located at: http://cio.idaho.gov/products_and_services/consolidated_messaging_project.htm
	• Also see: Desktop Support Services and Server Administration Services in the Service Catalog for further detail of the services that are provided.
	• Additional Services are also available through our Service Desk, as shown in this Service Catalog.
	
	EXCLUSIONS
	The following support services are not included and will not be provided:
	• Development, support, and maintenance of the Customer's web portal, web applications, and internal and external web sites;
	• Development, support, and maintenance of the Customer's custom applications;
	• Third-party applications;
	• Copiers; and
	• Database administration of MS SQL servers located at the Customer's location.

Service Level Objectives	**Service Levels:** Priority is set by determining how urgent the incident is, and what its immediate impact is. (See Support Services Service Agreement) **Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support is available for this service

	Scheduled Maintenance Window: Every Thursday 5:00PM – 7:00PM (Mountain Time) for all services and/or related components require regular maintenance.
Clients of the Service	Small agencies, boards, and commissions that do not have their own IT support personnel.
Business Processes Enabled by the Service	Information Technology and the support thereof enable an agency to conduct business effectively and efficiently.

Customer Roles and Responsibilities	• Contact the Service Desk to report problems;
	• Be available to identify the problem and work with the support technician;
	• Contact the helpdesk before making any changes to the system hardware or software;
	• Keep informed about the schedule of all planned network, hardware, and software changes and all major service related activities;
	• Take responsibility for educating users on a continuing basis about basic computer-related skills;
	• Maintain an updated version of virus protection software on all user systems at all times;
	• Maintain vulnerability patches and updates for non-operating system software as need arises;
	• Not install hardware or software without prior coordination with the Helpdesk. Hardware and software installations must only be performed by the helpdesk technicians or under the guidance of the helpdesk technicians;
	• Cover the costs for vendor technical support service calls for any off-the-shelf software in use by the Customer to resolve software support issues when the helpdesk technical staff need assistance from the software vendor to resolve a technical support problem with its software;
	• Advanced scheduling of all service related requests and other special services with the helpdesk.
	• When contacting the Helpdesk, provide the following information:
	  o Complete contact information (first and last name, e-mail address, agency, and telephone number);
	  o Type of computer on which the user is experiencing the problem (i.e., Dell Desktop or Laptop);
	  o The computer's operating system (e.g., Windows XP/Vista/windows 7); and
	  o A clear and specific description of the problem or request, including exact wording from any error messages received.
	• Adherence to all ICS policies; applicable ITRMC policies; State policies; Executive Orders; All applicable federal and local laws and regulations.

How to Access the Service	Services can be accessed by calling (208) 332-1500 and choosing option 3, sending email requests to helpdesk@cio.idaho.gov or by accessing the Service Desk at http://idaho.service-now.com
Cost Information	Cost is based on the number of desktop, laptops, printers, scanners, PDA's, and servers in use at the agency. For cost information contact the Support Services Manager: Carla Casper at – email: carla.casper@cio.idaho.gov, or phone: (208) 332-1853.

State of Idaho Office of the CIO Service Catalog – Support Services

Service Name	**Project Management Services**
Service Description	Provide IT project management services in the areas of Project Management, Portfolio Management, and External Services and Outreach Efforts.

Service Characteristics	• **Project Management –** Provide project management services to agencies and commissions that are provided IT support services by the Office of the CIO related to IT projects starting with the proposal state through the entire project management lifecycle.
	• **Portfolio Management –** Track large-scale IT projects in executive branch agencies. The IT portfolio management process is integrated into the state's IT budgeting and procurement processes to support the oversight and governance of information technology investments.
	• **External Services and Outreach Efforts –** Support the project management community throughout state government by providing resource information related to training and other services for project managers and government agencies. When needed, establish relationships and contracts with third-party vendors to provide project management services to agencies.
	• **Comprehensive Enterprise IT Project Management Information System -** Evaluate, prioritize, and select appropriate information technology investments for the State of Idaho by:
	  o Facilitating the exchange of project status information between agencies and the Office of the CIO
	  o Assisting in the assessment of project progress
	  o Improving the visibility and management of the state's portfolio of projects

Service Level Objectives	**Support Hours:** Normal Business Hours: Monday – Friday 7:00AM to 5:00PM (Mountain Time) NO after hours support is available for this service
Clients of the Service	• Small agencies, boards, and commissions that do not have their own IT support personnel. • Any state agency needing assistance with those areas of IT where they lack appropriate technical expertise. • The Information Technology Resource Management Council (ITRMC)
Business Processes Enabled by the Service	• Supporting state and agency strategic goals • Ensuring IT Services resources are allocated to the appropriate projects • Supporting best practice project management processes and procedures
Customer Roles and Responsibilities	• Where customers are involved in projects managed by OCIO Project Management Services, the customer will be expected to participate fully as designed into the project. • Adherence to all applicable ITRMC policies; State policies; Executive Orders; Applicable federal and local laws and regulations.
How to Access the Service	• Services can be accessed by sending email requests to: helpdesk@cio.idaho.gov , accessing the Service Desk at http://idaho.service-now.com, or by contacting any member of the Enterprise Plans and Programs Team. • P&P Team contact information is located at: http://cio.idaho.gov/customer_service/contact_list.htm
Cost Information	There are currently no costs associated with this service.

Appendix A: Incident vs. Service Request vs. Change Request

User Perspective

From the user's perspective there is no difference between a service request, an incident, or a change. All of the following are user requests, and can be requests for:

- support,
- delivery (of hardware or software, forms or other tangibles),
- information,
- advice,
- documentation,
- provisioning,
- a change in a process or procedure, or
- resolution to an IT problem.

Service Desk Perspective

From the Service Desk technician's perspective all of the above are also user requests; however, the first job of the service technician upon receiving a request of any kind from a user is to classify it as an incident, a change, or a Request for Service (Service Request).

A user's request becomes a Service Request if:

- It does not result in an interruption to service because of a failure in anything that supports the flow and processing of information, in other words, a failure in the IT Infrastructure,
- on initial inspection it does not require the need for a change to the IT infrastructure,
- for agencies using a CMDB, it does not require an update to the CMDB, and
- it does not change requested services.

Basic Example: A user requests a new profile be created in the ICS email system. This results in a change to the email profiles list, but not to the actual service which is provisioning, maintaining, securing, and delivering email services to users.

A Service Request is handled in the same way as an incident with many Service Desk tools, through the Incident Management process, and may bring about a change Request if research and review indicate a need for a change to infrastructure.

A user's request becomes an incident if it is a request or event which:

- is not part of the standard operation of service,
- causes or may cause an interruption to a service or operation, or
- causes a reduction in the quality of an operation, even if it has not yet impacted service.

An incident may bring about a change request if a resolution cannot be found within the boundaries of the current infrastructure, or if the resolution is a workaround to reestablish service quickly.

Basic Example: A user requests their email be fixed – it has been working with no problems, but suddenly stops. The email service has failed and the technician finds he must fix a corrupted profile by recreating it. The outcome is the same as in the service request example – an email profile is created – but this is an incident because it is initiated by a failure in the standard operation of email.

A user's request becomes a change request if:

- the technician determines it will require adding, modifying, improving, replacing, or removing any supported or baselined hardware, software, applications, or systems (network, environment, workstation and peripherals, etc.) and any associated documentation, or
- for agencies using a CMDB, it requires an update to the CMDB.

Example: All supported users' email will move to a new domain. There is no failure in service but the infrastructure baseline will change

Appendix B: ITIL Acronyms

V3, 30 May 2007

Acknowledgements

We would like to express our gratitude and acknowledge the contribution of Stuart Rance and Ashley Hanna of Hewlett-Packard in the production of this glossary.

Note for readers
This glossary may be freely downloaded. See **http://www.get-best-practice.co.uk/glossaries.aspx** for details of licence terms. Additions to this document specific to the State of Idaho are marked *'SoID'* to distinguish them from the original text. There is no affiliation nor implied endorsement by the official source below to the State of Idaho.

Official Source: "ITIL / PRINCE2 / M_o_R / Programme Management] Glossaries/Acronyms © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce"

"ITIL ® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office".

"PRINCE ® is a Registered Trade Mark and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office".

"M_o_R ® is a Registered Trade Mark and a Registered Community Trade Mark of the Office of Government Commerce".

Acronym	
ACD	Automatic Call Distribution
AM	Availability Management
AMIS	Availability Management Information System
ASP	Application Service Provider
BCM	Business Capacity Management
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BRM	Business Relationship Manager
BSI	British Standards Institution
BSM	Business Service Management
CAB	Change Advisory Board
CAB/EC	Change Advisory Board / Emergency Committee
CAPEX	Capital Expenditure
CCM	Component Capacity Management
CFIA	Component Failure Impact Analysis
CI	Configuration Item
CMDB	Configuration Management Database
CMIS	Capacity Management Information System
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CMS	Configuration Management System
COTS	Commercial off the Shelf
CSF	Critical Success Factor
CSI	Continual Service Improvement
CSIP	Continual Service Improvement Programme
CSP	Core Service Package
CTI	Computer Telephony Integration
DIKW	Data-to-Information-to-Knowledge-to-Wisdom
eSCM-CL	eSourcing Capability Model for Client Organizations
eSCM-SP	eSourcing Capability Model for Service Providers

Acronym	
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
IRR	Internal Rate of Return
ISG	IT Steering Group
ISM	Information Security Management
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITSCM	IT Service Continuity Management
ITSM	IT Service Management
itSMF	IT Service Management Forum
IVR	Interactive Voice Response
KEDB	Known Error Database
KPI	Key Performance Indicator
LOS	Line of Service
MoR	Management of Risk
MTBF	Mean Time Between Failures
MOA (SofID)	***Memorandum of Agreement***
MTBSI	Mean Time Between Service Incidents
MTRS	Mean Time to Restore Service
MTTR	Mean Time to Repair
NPV	Net Present Value
OGC	Office of Government Commerce
OLA	Operational Level Agreement
OPEX	Operational Expenditure
OPSI	Office of Public Sector Information
PBA	Pattern of Business Activity
PFS	Prerequisite for Success

Acronym	
PIR	Post Implementation Review
PSA	Projected Service Availability
QA	Quality Assurance
QMS	Quality Management System
RCA	Root Cause Analysis
RFC	Request for Change
ROI	Return on Investment
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAC	Service Acceptance Criteria
SACM	Service Asset and Configuration Management
SCD	Supplier and Contract Database
SCM	Service Capacity Management
SFA	Service Failure Analysis
SIP	Service Improvement Plan
SKMS	Service Knowledge Management System
SLA	Service Level Agreement (see MOA)
SLM	Service Level Management
SLP	Service Level Package
SLR	Service Level Requirement
SMO	Service Maintenance Objective
SoC	Separation of Concerns
SOP	Standard Operating Procedures
SOR	Statement of requirements
SPI	Service Provider Interface
SPM	Service Portfolio Management
SPO	Service Provisioning Optimization
SPOF	Single Point of Failure
TCO	Total Cost of Ownership
TCU	Total Cost of Utilization

Acronym	
TO	Technical Observation
TOR	Terms of Reference
TQM	Total Quality Management
UC	Underpinning Contract
UP	User Profile
VBF	Vital Business Function
VOI	Value on Investment
WIP	Work in Progress

Appendix C: ITIL Glossary of Terms

V3, 30 May 2007

Acknowledgements

We would like to express our gratitude and acknowledge the contribution of Stuart Rance and Ashley Hanna of Hewlett-Packard in the production of this glossary.

Note for readers
This glossary may be freely downloaded. See **http://www.get-best-practice.co.uk/glossaries.aspx** for details of licence terms. Additions to this document specific to the State of Idaho are marked *'SoID'* to distinguish them from the original text. There is no affiliation nor implied endorsement by the official source below to the State of Idaho.

Source: "ITIL / PRINCE2 / M_o_R / Programme Management] Glossaries/Acronyms © Crown Copyright Office of Government Commerce. Reproduced with the permission of the Controller of HMSO and the Office of Government Commerce"

"ITIL ® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office".

"PRINCE ® is a Registered Trade Mark and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office".

"M_o_R ® is a Registered Trade Mark and a Registered Community Trade Mark of the Office of Government Commerce".

Term	Definition
Acceptance	Formal agreement that an IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and meets its specified Requirements. Acceptance is usually preceded by Evaluation or Testing and is often required before proceeding to the next stage of a Project or Process. See Service Acceptance Criteria.
Access Management	**(Service Operation)** The Process responsible for allowing Users to make use of IT Services, data, or other Assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized Users are able to access or modify the Assets. Access Management is sometimes referred to as Rights Management or Identity Management.
Account Manager	**(Service Strategy)** A Role that is very similar to Business Relationship Manager, but includes more commercial aspects. Most commonly used when dealing with External Customers.
Accounting	**(Service Strategy)** The Process responsible for identifying actual Costs of delivering IT Services, comparing these with budgeted costs, and managing variance from the Budget.
Accredited	Officially authorised to carry out a Role. For example an Accredited body may be authorised to provide training or to conduct Audits.
Active Monitoring	**(Service Operation)** Monitoring of a Configuration Item or an IT Service that uses automated regular checks to discover the current status. See Passive Monitoring.
Activity	A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or Plans, and are documented in Procedures.
Agreed Service Time	**(Service Design)** A synonym for Service Hours, commonly used in formal calculations of Availability. See Downtime.
Agreement	A Document that describes a formal understanding between two or more parties. An Agreement is not legally binding, unless it forms part of a Contract. See Service Level Agreement, Operational Level Agreement.
Alert	**(Service Operation)** A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.
Analytical Modelling	**(Service Strategy) (Service Design) (Continual Service Improvement)** A technique that uses mathematical Models to predict the behaviour of a Configuration Item or IT Service. Analytical Models are commonly used in Capacity Management and Availability Management. See Modelling.
Application	Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Service. An Application runs on one or more Servers or Clients. See Application Management, Application Portfolio.
Application Management	**(Service Design) (Service Operation)** The Function responsible for managing Applications throughout their Lifecycle.
Application Portfolio	(Service Design) A database or structured Document used to manage Applications throughout their Lifecycle. The Application Portfolio contains key

Term	Definition
	Attributes of all Applications. The Application Portfolio is sometimes implemented as part of the Service Portfolio, or as part of the Configuration Management System.
Application Service Provider (ASP)	**(Service Design)** An External Service Provider that provides IT Services using Applications running at the Service Provider's premises. Users access the Applications by network connections to the Service Provider.
Application Sizing	**(Service Design)** The Activity responsible for understanding the Resource Requirements needed to support a new Application, or a major Change to an existing Application. Application Sizing helps to ensure that the IT Service can meet its agreed Service Level Targets for Capacity and Performance.
Architecture	**(Service Design)** The structure of a System or IT Service, including the Relationships of Components to each other and to the environment they are in. Architecture also includes the Standards and Guidelines which guide the design and evolution of the System.
Assembly	**(Service Transition)** A Configuration Item that is made up from a number of other CIs. For example a Server CI may contain CIs for CPUs, Disks, Memory etc.; an IT Service CI may contain many Hardware, Software and other CIs. See Component CI, Build.
Assessment	Inspection and analysis to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. See Audit.
Asset	**(Service Strategy)** Any Resource or Capability. Assets of a Service Provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organisation, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.
Asset Management	**(Service Transition)** Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process. See Asset Register.
Asset Register	**(Service Transition)** A list of Assets, which includes their ownership and value. The Asset Register is maintained by Asset Management.
Attribute	**(Service Transition)** A piece of information about a Configuration Item. Examples are name, location, Version number, and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB). See Relationship.
Audit	Formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups. See Certification, Assessment.
Authority Matrix	Synonym for RACI.
Automatic Call Distribution	**(Service Operation)** Use of Information Technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD

Term	Definition
(ACD)	is sometimes called Automated Call Distribution.
Availability	**(Service Design)** Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service.
Availability Management	**(Service Design)** The Process responsible for defining, analysing, Planning, measuring and improving all aspects of the Availability of IT Services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, Tools, Roles etc are appropriate for the agreed Service Level Targets for Availability.
Availability Management Information System (AMIS)	**(Service Design)** A virtual repository of all Availability Management data, usually stored in multiple physical locations. See Service Knowledge Management System.
Availability Plan	**(Service Design)** A Plan to ensure that existing and future Availability Requirements for IT Services can be provided Cost Effectively.
Back-out	Synonym for Remediation.
Backup	**(Service Design) (Service Operation)** Copying data to protect against loss of Integrity or Availability of the original.
Balanced Scorecard	**(Continual Service Improvement)** A management tool developed by Drs. Robert Kaplan (Harvard Business School) and David Norton. A Balanced Scorecard enables a Strategy to be broken down into Key Performance Indicators. Performance against the KPIs is used to demonstrate how well the Strategy is being achieved. A Balanced Scorecard has 4 major areas, each of which has a small number of KPIs. The same 4 areas are considered at different levels of detail throughout the Organisation.
Baseline	**(Continual Service Improvement)** A Benchmark used as a reference point. For example: • An ITSM Baseline can be used as a starting point to measure the effect of a Service Improvement Plan • A Performance Baseline can be used to measure changes in Performance over the lifetime of an IT Service • A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known Configuration if a Change or Release fails
Benchmark	**(Continual Service Improvement)** The recorded state of something at a specific point in time. A Benchmark can be created for a Configuration, a Process, or any other set of data. For example, a benchmark can be used in: • Continual Service Improvement, to establish the current state for managing improvements. • Capacity Management, to document Performance characteristics during normal

Term	Definition
	operations. • See Benchmarking, Baseline.
Benchmarking	**(Continual Service Improvement)** Comparing a Benchmark with a Baseline or with Best Practice. The term Benchmarking is also used to mean creating a series of Benchmarks over time, and comparing the results to measure progress or improvement.
Best Practice	Proven Activities or Processes that have been successfully used by multiple Organisations. ITIL is an example of Best Practice.
Brainstorming	**(Service Design)** A technique that helps a team to generate ideas. Ideas are not reviewed during the Brainstorming session, but at a later stage. Brainstorming is often used by Problem Management to identify possible causes.
British Standards Institution (BSI)	The UK National Standards body, responsible for creating and maintaining British Standards. See http://www.bsi-global.com for more information. See ISO.
Budget	A list of all the money an Organisation or Business Unit plans to receive, and plans to pay out, over a specified period of time. See Budgeting, Planning.
Budgeting	The Activity of predicting and controlling the spending of money. Consists of a periodic negotiation cycle to set future Budgets (usually annual) and the day-to-day monitoring and adjusting of current Budgets.
Build	**(Service Transition)** The Activity of assembling a number of Configuration Items to create part of an IT Service. The term Build is also used to refer to a Release that is authorised for distribution. For example Server Build or laptop Build. See Configuration Baseline.
Build Environment	**(Service Transition)** A controlled Environment where Applications, IT Services and other Builds are assembled prior to being moved into a Test or Live Environment.
Business	**(Service Strategy)** An overall corporate entity or Organisation formed of a number of Business Units. In the context of ITSM, the term Business includes public sector and not-for-profit organisations, as well as companies. An IT Service Provider provides IT Services to a Customer within a Business. The IT Service Provider may be part of the same Business as their Customer (Internal Service Provider), or part of another Business (External Service Provider).
Business Capacity Management (BCM)	**(Service Design)** In the context of ITSM, Business Capacity Management is the Activity responsible for understanding future Business Requirements for use in the Capacity Plan. See Service Capacity Management.
Business Case	**(Service Strategy)** Justification for a significant item of expenditure. Includes information about Costs, benefits, options, issues, Risks, and possible problems. See Cost Benefit Analysis.
Business Continuity Management	**(Service Design)** The Business Process responsible for managing Risks that could seriously impact the Business. BCM safeguards the interests of key stakeholders, reputation, brand and value creating activities. The BCM Process

Term	Definition
(BCM)	involves reducing Risks to an acceptable level and planning for the recovery of Business Processes should a disruption to the Business occur. BCM sets the Objectives, Scope and Requirements for IT Service Continuity Management.
Business Continuity Plan (BCP)	**(Service Design)** A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. IT Service Continuity Plans form a significant part of Business Continuity Plans.
Business Customer	**(Service Strategy)** A recipient of a product or a Service from the Business. For example if the Business is a car manufacturer then the Business Customer is someone who buys a car.
Business Impact Analysis (BIA)	**(Service Strategy)** BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other Business Processes, IT Services etc. BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.
Business Objective	**(Service Strategy)** The Objective of a Business Process, or of the Business as a whole. Business Objectives support the Business Vision, provide guidance for the IT Strategy, and are often supported by IT Services.
Business Operations	**(Service Strategy)** The day-to-day execution, monitoring and management of Business Processes.
Business Perspective	**(Continual Service Improvement)** An understanding of the Service Provider and IT Services from the point of view of the Business, and an understanding of the Business from the point of view of the Service Provider.
Business Process	A Process that is owned and carried out by the Business. A Business Process contributes to the delivery of a product or Service to a Business Customer. For example, a retailer may have a purchasing Process which helps to deliver Services to their Business Customers. Many Business Processes rely on IT Services.
Business Relationship Management	**(Service Strategy)** The Process or Function responsible for maintaining a Relationship with the Business. BRM usually includes: • Managing personal Relationships with Business managers • Providing input to Service Portfolio Management • Ensuring that the IT Service Provider is satisfying the Business needs of the Customers This Process has strong links with Service Level Management.
Business Relationship Manager (BRM)	**(Service Strategy)** A Role responsible for maintaining the Relationship with one or more Customers. This Role is often combined with the Service Level Manager Role. See Account Manager.
Business Service	An IT Service that directly supports a Business Process, as opposed to an Infrastructure Service which is used internally by the IT Service Provider and is not usually visible to the Business. The term Business Service is also used to mean a Service that is delivered to

Term	Definition
	Business Customers by Business Units. For example delivery of financial services to Customers of a bank, or goods to the Customers of a retail store. Successful delivery of Business Services often depends on one or more IT Services.
Business Service Management (BSM)	**(Service Strategy) (Service Design)** An approach to the management of IT Services that considers the Business Processes supported and the Business value provided. This term also means the management of Business Services delivered to Business Customers.
Business Unit	**(Service Strategy)** A segment of the Business which has its own Plans, Metrics, income and Costs. Each Business Unit owns Assets and uses these to create value for Customers in the form of goods and Services.
Call	**(Service Operation)** A telephone call to the Service Desk from a User. A Call could result in an Incident or a Service Request being logged.
Call Centre	**(Service Operation)** An Organisation or Business Unit which handles large numbers of incoming and outgoing telephone calls. See Service Desk.
Call Type	**(Service Operation)** A Category that is used to distinguish incoming requests to a Service Desk. Common Call Types are Incident, Service Request and Complaint.
Capability	**(Service Strategy)** The ability of an Organisation, person, Process, Application, Configuration Item or IT Service to carry out an Activity. Capabilities are intangible Assets of an Organisation. See Resource.
Capability Maturity Model (CMM)	**(Continual Service Improvement)** The Capability Maturity Model for Software (also known as the CMM and SW-CMM) is a model used to identify Best Practices to help increase Process Maturity. CMM was developed at the Software Engineering Institute (SEI) of Carnegie Mellon University. In 2000, the SW-CMM was upgraded to CMMI® (Capability Maturity Model Integration). The SEI no longer maintains the SW-CMM model, its associated appraisal methods, or training materials.
Capability Maturity Model Integration (CMMI)	**(Continual Service Improvement)** Capability Maturity Model® Integration (CMMI) is a process improvement approach developed by the Software Engineering Institute (SEI) of Carnegie Melon University. CMMI provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division, or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. See http://www.sei.cmu.edu/cmmi/ for more information. See CMM, Continuous Improvement, Maturity.
Capacity	**(Service Design)** The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.
Capacity Management	**(Service Design)** The Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets

Term	Definition
	in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long term Business Requirements.
Capacity Management Information System (CMIS)	**(Service Design)** A virtual repository of all Capacity Management data, usually stored in multiple physical locations. See Service Knowledge Management System.
Capacity Plan	**(Service Design)** A Capacity Plan is used to manage the Resources required to deliver IT Services. The Plan contains scenarios for different predictions of Business demand, and costed options to deliver the agreed Service Level Targets.
Capacity Planning	**(Service Design)** The Activity within Capacity Management responsible for creating a Capacity Plan.
Capital Expenditure (CAPEX)	**(Service Strategy)** The Cost of purchasing something that will become a financial Asset, for example computer equipment and buildings. The value of the Asset is Depreciated over multiple accounting periods.
Capital Item	**(Service Strategy)** An Asset that is of interest to Financial Management because it is above an agreed financial value.
Capitalization	**(Service Strategy)** Identifying major Cost as capital, even though no Asset is purchased. This is done to spread the impact of the Cost over multiple accounting periods. The most common example of this is software development, or purchase of a software license.
Category	A named group of things that have something in common. Categories are used to group similar things together. For example Cost Types are used to group similar types of Cost. Incident Categories are used to group similar types of Incident, CI Types are used to group similar types of Configuration Item.
Certification	Issuing a certificate to confirm Compliance to a Standard. Certification includes a formal Audit by an independent and Accredited body. The term Certification is also used to mean awarding a certificate to verify that a person has achieved a qualification.
Change	**(Service Transition)** The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Processes, Documentation etc.
Change Advisory Board (CAB)	**(Service Transition)** A group of people that advises the Change Manager in the Assessment, prioritisation and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, the Business, and Third Parties such as Suppliers.
Change Case	**(Service Operation)** A technique used to predict the impact of proposed Changes. Change Cases use specific scenarios to clarify the scope of proposed Changes and to help with Cost Benefit Analysis. See Use Case.
Change History	**(Service Transition)** Information about all changes made to a Configuration Item during its life. Change History consists of all those Change Records that apply to the CI.

Term	Definition
Change Management	**(Service Transition)** The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.
Change Model	**(Service Transition)** A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a Change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software Release). See Standard Change, Change Advisory Board.
Change Record	**(Service Transition)** A Record containing the details of a Change. Each Change Record documents the Lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.
Change Request	Synonym for Request for Change.
Change Schedule	**(Service Transition)** A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.
Change Window	**(Service Transition)** A regular, agreed time when Changes or Releases may be implemented with minimal impact on Services. Change Windows are usually documented in SLAs.
Charging	**(Service Strategy)** Requiring payment for IT Services. Charging for IT Services is optional, and many Organisations choose to treat their IT Service Provider as a Cost Centre.
Chronological Analysis	**(Service Operation)** A technique used to help identify possible causes of Problems. All available data about the Problem is collected and sorted by date and time to provide a detailed timeline. This can make it possible to identify which Events may have been triggered by others.
CI Type	**(Service Transition)** A Category that is used to Classify CIs. The CI Type identifies the required Attributes and Relationships for a Configuration Record. Common CI Types include: hardware, Document, User etc.
Classification	The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes etc. are usually classified.
Client	A generic term that means a Customer, the Business or a Business Customer. For example Client Manager may be used as a synonym for Account Manager. The term client is also used to mean: • A computer that is used directly by a User, for example a PC, Handheld Computer, or Workstation. • The part of a Client-Server Application that the User directly interfaces with. For example an email Client.
Closed	**(Service Operation)** The final Status in the Lifecycle of an Incident, Problem,

Term	Definition
	Change etc. When the Status is Closed, no further action is taken.
Closure	**(Service Operation)** The act of changing the Status of an Incident, Problem, Change etc. to Closed.
COBIT	**(Continual Service Improvement)** Control Objectives for Information and related Technology (COBIT) provides guidance and Best Practice for the management of IT Processes. COBIT is published by the IT Governance Institute. See http://www.isaca.org/ for more information.
Code of Practice	A Guideline published by a public body or a Standards Organisation, such as ISO or BSI. Many Standards consist of a Code of Practice and a Specification. The Code of Practice describes recommended Best Practice.
Cold Standby	Synonym for Gradual Recovery.
Commercial off the Shelf (COTS)	**(Service Design)** Application software or Middleware that can be purchased from a Third Party.
Compliance	Ensuring that a Standard or set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed.
Component	A general term that is used to mean one part of something more complex. For example, a computer System may be a component of an IT Service, an Application may be a Component of a Release Unit. Components that need to be managed should be Configuration Items.
Component Capacity Management (CCM)	**(Service Design) (Continual Service Improvement)** The Process responsible for understanding the Capacity, Utilisation, and Performance of Configuration Items. Data is collected, recorded and analysed for use in the Capacity Plan. See Service Capacity Management.
Component CI	**(Service Transition)** A Configuration Item that is part of an Assembly. For example, a CPU or Memory CI may be part of a Server CI.
Component Failure Impact Analysis (CFIA)	**(Service Design)** A technique that helps to identify the impact of CI failure on IT Services. A matrix is created with IT Services on one edge and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT Services) and of fragile IT Services (that have multiple Single Points of Failure).
Computer Telephony Integration (CTI)	**(Service Operation)** CTI is a general term covering any kind of integration between computers and telephone Systems. It is most commonly used to refer to Systems where an Application displays detailed screens relating to incoming or outgoing telephone calls. See Automatic Call Distribution, Interactive Voice Response.
Concurrency	A measure of the number of Users engaged in the same Operation at the same time.
Confidentiality	**(Service Design)** A security principle that requires that data should only be accessed by authorised people.
Configuration	**(Service Transition)** A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.

Term	Definition
Configuration Baseline	**(Service Transition)** A Baseline of a Configuration that has been formally agreed and is managed through the Change Management process. A Configuration Baseline is used as a basis for future Builds, Releases and Changes.
Configuration Control	**(Service Transition)** The Activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request.
Configuration Identification	**(Service Transition)** The Activity responsible for collecting information about Configuration Items and their Relationships, and loading this information into the CMDB. Configuration Identification is also responsible for labelling the CIs themselves, so that the corresponding Configuration Records can be found.
Configuration Item (CI)	**(Service Transition)** Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.
Configuration Management	**(Service Transition)** The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.
Configuration Management Database (CMDB)	**(Service Transition)** A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.
Configuration Management System (CMS)	**(Service Transition)** A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See Configuration Management Database, Service Knowledge Management System.
Configuration Record	**(Service Transition)** A Record containing the details of a Configuration Item. Each Configuration Record documents the Lifecycle of a single CI. Configuration Records are stored in a Configuration Management Database.
Configuration Structure	**(Service Transition)** The hierarchy and other Relationships between all the Configuration Items that comprise a Configuration.
Continual Service Improvement (CSI)	**(Continual Service Improvement)** A stage in the Lifecycle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The Performance of the IT Service Provider is continually measured and improvements are made to

Term	Definition
	Processes, IT Services and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See Plan-Do-Check-Act.
Continuous Availability	**(Service Design)** An approach or design to achieve 100% Availability. A Continuously Available IT Service has no planned or unplanned Downtime.
Continuous Operation	**(Service Design)** An approach or design to eliminate planned Downtime of an IT Service. Note that individual Configuration Items may be down even though the IT Service is Available.
Contract	A legally binding Agreement between two or more parties.
Contract Portfolio	**(Service Strategy)** A database or structured Document used to manage Service Contracts or Agreements between an IT Service Provider and their Customers. Each IT Service delivered to a Customer should have a Contract or other Agreement which is listed in the Contract Portfolio. See Service Portfolio, Service Catalogue.
Control	A means of managing a Risk, ensuring that a Business Objective is achieved, or ensuring that a Process is followed. Example Controls include Policies, Procedures, Roles, RAID, door-locks etc. A control is sometimes called a Countermeasure or safeguard. Control also means to manage the utilization or behaviour of a Configuration Item, System or IT Service.
Control Objectives for Information and related Technology (COBIT)	See COBIT.
Control perspective	**(Service Strategy)** An approach to the management of IT Services, Processes, Functions, Assets etc. There can be several different Control Perspectives on the same IT Service, Process etc., allowing different individuals or teams to focus on what is important and relevant to their specific Role. Example Control Perspectives include Reactive and Proactive management within IT Operations, or a Lifecycle view for an Application Project team.
Control Processes	The ISO/IEC 20000 Process group that includes Change Management and Configuration Management.
Core Service	**(Service Strategy)** An IT Service that delivers basic Outcomes desired by one or more Customers. See Supporting Service, Core Service Package.
Core Service Package (CSP)	**(Service Strategy)** A detailed description of a Core Service that may be shared by two or more Service Level Packages. See Service Package.
Cost	The amount of money spent on a specific Activity, IT Service, or Business Unit. Costs consist of real cost (money), notional cost such as people's time, and Depreciation.
Cost Benefit Analysis	An Activity that analyses and compares the Costs and the benefits involved in one or more alternative courses of action.

Term	Definition
	See Business Case, Net Present Value, Internal Rate of Return, Return on Investment, Value on Investment.
Cost Centre	**(Service Strategy)** A Business Unit or Project to which Costs are assigned. A Cost Centre does not charge for Services provided. An IT Service Provider can be run as a Cost Centre or a Profit Centre.
Cost Effectiveness	A measure of the balance between the Effectiveness and Cost of a Service, Process or activity, A Cost Effective Process is one which achieves its Objectives at minimum Cost. See KPI, Return on Investment, Value for Money.
Cost Element	**(Service Strategy)** The middle level of category to which Costs are assigned in Budgeting and Accounting. The highest level category is Cost Type. For example a Cost Type of “people” could have cost elements of payroll, staff benefits, expenses, training, overtime etc. Cost Elements can be further broken down to give Cost Units. For example the Cost Element “expenses” could include Cost Units of Hotels, Transport, Meals etc.
Cost Management	**(Service Strategy)** A general term that is used to refer to Budgeting and Accounting, sometimes used as a synonym for Financial Management
Cost Type	**(Service Strategy)** The highest level of category to which Costs are assigned in Budgeting and Accounting. For example hardware, software, people, accommodation, external and Transfer. See Cost Element, Cost Type.
Cost Unit	**(Service Strategy)** The lowest level of category to which Costs are assigned, Cost Units are usually things that can be easily counted (e.g. staff numbers, software licences) or things easily measured (e.g. CPU usage, Electricity consumed). Cost Units are included within Cost Elements. For example a Cost Element of “expenses” could include Cost Units of Hotels, Transport, Meals etc. See Cost Type.
Countermeasure	Can be used to refer to any type of Control. The term Countermeasure is most often used when referring to measures that increase Resilience, Fault Tolerance or Reliability of an IT Service.
Course Corrections	Changes made to a Plan or Activity that has already started, to ensure that it will meet its Objectives. Course corrections are made as a result of Monitoring progress.
CRAMM	A methodology and tool for analysing and managing Risks. CRAMM was developed by the UK Government, but is now privately owned. Further information is available from http://www.cramm.com/
Crisis Management	The Process responsible for managing the wider implications of Business Continuity. A Crisis Management team is responsible for Strategic issues such as managing media relations and shareholder confidence, and decides when to invoke Business Continuity Plans.
Critical Success Factor (CSF)	Something that must happen if a Process, Project, Plan, or IT Service is to succeed. KPIs are used to measure the achievement of each CSF. For example a CSF of "protect IT Services when making Changes" could be measured by KPIs such as "percentage reduction of unsuccessful Changes", "percentage reduction in Changes causing Incidents" etc.

Term	Definition
Culture	A set of values that is shared by a group of people, including expectations about how people should behave, ideas, beliefs, and practices. See Vision.
Customer	Someone who buys goods or Services. The Customer of an IT Service Provider is the person or group who defines and agrees the Service Level Targets. The term Customers is also sometimes informally used to mean Users, for example "this is a Customer focussed Organisation".
Customer Portfolio	**(Service Strategy)** A database or structured Document used to record all Customers of the IT Service Provider. The Customer Portfolio is the Business Relationship Manager's view of the Customers who receive Services from the IT Service Provider. See Contract Portfolio, Service Portfolio.
Dashboard	**(Service Operation)** A graphical representation of overall IT Service Performance and Availability. Dashboard images may be updated in real-time, and can also be included in management reports and web pages. Dashboards can be used to support Service Level Management, Event Management or Incident Diagnosis.
Data-to-Information-to-Knowledge-to-Wisdom (DIKW)	A way of understanding the relationships between data, information, knowledge, and wisdom. DIKW shows how each of these builds on the others.
Definitive Media Library (DML)	**(Service Transition)** One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DML may also contain associated CIs such as licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of Change and Release Management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a Release.
Deliverable	Something that must be provided to meet a commitment in a Service Level Agreement or a Contract. Deliverable is also used in a more informal way to mean a planned output of any Process.
Demand Management	Activities that understand and influence Customer demand for Services and the provision of Capacity to meet these demands. At a Strategic level Demand Management can involve analysis of Patterns of Business Activity and User Profiles. At a Tactical level it can involve use of Differential Charging to encourage Customers to use IT Services at less busy times. See Capacity Management.
Deming Cycle	Synonym for Plan Do Check Act.
Dependency	The direct or indirect reliance of one Process or Activity upon another.
Deployment	**(Service Transition)** The Activity responsible for movement of new or changed hardware, software, documentation, Process, etc to the Live Environment. Deployment is part of the Release and Deployment Management Process. See Rollout.
Depreciation	**(Service Strategy)** A measure of the reduction in value of an Asset over its life. This is based on wearing out, consumption or other reduction in the useful

Term	Definition
	economic value.
Design	**(Service Design)** An Activity or Process that identifies Requirements and then defines a solution that is able to meet these Requirements. See Service Design.
Detection	**(Service Operation)** A stage in the Incident Lifecycle. Detection results in the Incident becoming known to the Service Provider. Detection can be automatic, or can be the result of a User logging an Incident.
Development	**(Service Design)** The Process responsible for creating or modifying an IT Service or Application. Also used to mean the Role or group that carries out Development work.
Development Environment	**(Service Design)** An Environment used to create or modify IT Services or Applications. Development Environments are not typically subjected to the same degree of control as Test Environments or Live Environments. See Development.
Diagnosis	**(Service Operation)** A stage in the Incident and Problem Lifecycles. The purpose of Diagnosis is to identify a Workaround for an Incident or the Root Cause of a Problem.
Diagnostic Script	**(Service Operation)** A structured set of questions used by Service Desk staff to ensure they ask the correct questions, and to help them Classify, Resolve and assign Incidents. Diagnostic Scripts may also be made available to Users to help them diagnose and resolve their own Incidents.
Differential Charging	A technique used to support Demand Management by charging different amounts for the same IT Service Function at different times.
Direct Cost	**(Service Strategy)** A cost of providing an IT Service which can be allocated in full to a specific Customer, Cost Centre, Project etc. For example cost of providing non-shared servers or software licenses. See Indirect Cost.
Directory Service	**(Service Operation)** An Application that manages information about IT Infrastructure available on a network, and corresponding User access Rights.
Do Nothing	**(Service Design)** A Recovery Option. The Service Provider formally agrees with the Customer that Recovery of this IT Service will not be performed.
Document	Information in readable form. A Document may be paper or electronic. For example a Policy statement, Service Level Agreement, Incident Record, diagram of computer room layout. See Record.
Downtime	**(Service Design) (Service Operation)** The time when a Configuration Item or IT Service is not Available during its Agreed Service Time. The Availability of an IT Service is often calculated from Agreed Service Time and Downtime.
Driver	Something that influences Strategy, Objectives or Requirements. For example new legislation or the actions of competitors.
Early Life Support	**(Service Transition)** Support provided for a new or Changed IT Service for a period of time after it is Released. During Early Life Support the IT Service Provider may review the KPIs, Service Levels and Monitoring Thresholds, and

Term	Definition
	provide additional Resources for Incident and Problem Management.
Economies of scale	**(Service Strategy)** The reduction in average Cost that is possible from increasing the usage of an IT Service or Asset. See Economies of Scope.
Economies of scope	**(Service Strategy)** The reduction in Cost that is allocated to an IT Service by using an existing Asset for an additional purpose. For example delivering a new IT Service from existing IT Infrastructure. See Economies of Scale.
Effectiveness	**(Continual Service Improvement)** A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or Activity is one that achieves its agreed Objectives. See KPI.
Efficiency	**(Continual Service Improvement)** A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. See KPI.
Emergency Change	**(Service Transition)** A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes. See Emergency Change Advisory Board (ECAB).
Emergency Change Advisory Board (ECAB)	**(Service Transition)** A sub-set of the Change Advisory Board who make decisions about high impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.
Environment	**(Service Transition)** A subset of the IT Infrastructure that is used for a particular purpose. For Example: Live Environment, Test Environment, Build Environment. It is possible for multiple Environments to share a Configuration Item, for example Test and Live Environments may use different partitions on a single mainframe computer. Also used in the term Physical Environment to mean the accommodation, air conditioning, power system etc. Environment is also used as a generic term to mean the external conditions that influence or affect something.
Error	**(Service Operation)** A design flaw or malfunction that causes a Failure of one or more Configuration Items or IT Services. A mistake made by a person or a faulty Process that impacts a CI or IT Service is also an Error.
Escalation	**(Service Operation)** An Activity that obtains additional Resources when these are needed to meet Service Level Targets or Customer expectations. Escalation may be needed within any IT Service Management Process, but is most commonly associated with Incident Management, Problem Management and the management of Customer complaints. There are two types of Escalation, Functional Escalation and Hierarchic Escalation.
eSourcing Capability Model for Client	**(Service Strategy)** A framework to help Organisations guide their analysis and decisions on Service Sourcing Models and Strategies. eSCM-CL was developed by Carnegie Mellon University.

Term	Definition
Organizations (eSCM-CL)	See eSCM-SP.
eSourcing Capability Model for Service Providers (eSCM-SP)	**(Service Strategy)** A framework to help IT Service Providers develop their IT Service Management Capabilities from a Service Sourcing perspective. eSCM-SP was developed by Carnegie Mellon University. See eSCM-CL.
Estimation	The use of experience to provide an approximate value for a Metric or Cost. Estimation is also used in Capacity and Availability Management as the cheapest and least accurate Modelling method.
Evaluation	**(Service Transition)** The Process responsible for assessing a new or Changed IT Service to ensure that Risks have been managed and to help determine whether to proceed with the Change. Evaluation is also used to mean comparing an actual Outcome with the intended Outcome, or comparing one alternative with another.
Event	**(Service Operation)** A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.
Event Management	**(Service Operation)** The Process responsible for managing Events throughout their Lifecycle. Event Management is one of the main Activities of IT Operations.
Exception Report	A Document containing details of one or more KPIs or other important targets that have exceeded defined Thresholds. Examples include SLA targets being missed or about to be missed, and a Performance Metric indicating a potential Capacity problem.
Expanded Incident Lifecycle	**(Availability Management)** Detailed stages in the Lifecycle of an Incident. The stages are Detection, Diagnosis, Repair, Recovery, Restoration. The Expanded Incident Lifecycle is used to help understand all contributions to the Impact of Incidents and to Plan how these could be controlled or reduced.
External Customer	A Customer who works for a different Business to the IT Service Provider. See External Service Provider, Internal Customer.
External Metric	A Metric that is used to measure the delivery of IT Service to a Customer. External Metrics are usually defined in SLAs and reported to Customers. See Internal Metric.
External Service Provider	**(Service Strategy)** An IT Service Provider which is part of a different Organisation to their Customer. An IT Service Provider may have both Internal Customers and External Customers. See Type III Service Provider.
External Sourcing	Synonym for Outsourcing.
Facilities Management	**(Service Operation)** The Function responsible for managing the physical Environment where the IT Infrastructure is located. Facilities Management includes all aspects of managing the physical Environment, for example power and cooling, building Access Management, and environmental Monitoring.

Term	Definition
Failure	**(Service Operation)** Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, Configuration Items etc. A Failure often causes an Incident.
Failure Modes and Effects Analysis (FMEA)	An approach to assessing the potential Impact of Failures. FMEA involves analysing what would happen after Failure of each Configuration Item, all the way up to the effect on the Business. FMEA is often used in Information Security Management and in IT Service Continuity Planning.
Fast Recovery	**(Service Design)** A Recovery Option which is also known as Hot Standby. Provision is made to Recover the IT Service in a short period of time, typically less than 24 hours. Fast Recovery typically uses a dedicated Fixed Facility with computer Systems, and software configured ready to run the IT Services. Immediate Recovery may take up to 24 hours if there is a need to Restore data from Backups.
Fault	Synonym for Error.
Fault Tolerance	**(Service Design)** The ability of an IT Service or Configuration Item to continue to Operate correctly after Failure of a Component part. See Resilience, Countermeasure.
Fault Tree Analysis (FTA)	**(Service Design) (Continual Service Improvement)** A technique that can be used to determine the chain of Events that leads to a Problem. Fault Tree Analysis represents a chain of Events using Boolean notation in a diagram.
Financial Management	**(Service Strategy)** The Function and Processes responsible for managing an IT Service Provider's Budgeting, Accounting and Charging Requirements.
First-line Support	**(Service Operation)** The first level in a hierarchy of Support Groups involved in the resolution of Incidents. Each level contains more specialist skills, or has more time or other Resources. See Escalation.
Fishbone Diagram	Synonym for Ishikawa Diagram.
Fit for Purpose	An informal term used to describe a Process, Configuration Item, IT Service etc. that is capable of meeting its Objectives or Service Levels. Being Fit for Purpose requires suitable Design, implementation, Control and maintenance.
Fixed Cost	**(Service Strategy)** A Cost that does not vary with IT Service usage. For example the cost of Server hardware. See Variable Cost.
Fixed Facility	**(Service Design)** A permanent building, available for use when needed by an IT Service Continuity Plan. See Recovery Option, Portable Facility.
Follow the Sun	**(Service Operation)** A methodology for using Service Desks and Support Groups around the world to provide seamless 24 * 7 Service. Calls, Incidents, Problems and Service Requests are passed between groups in different time zones.
Fulfilment	Performing Activities to meet a need or Requirement. For example by providing a new IT Service, or meeting a Service Request.

Term	Definition
Function	A team or group of people and the tools they use to carry out one or more Processes or Activities. For example the Service Desk. The term Function also has two other meanings • An intended purpose of a Configuration Item, Person, Team, Process, or IT Service. For example one Function of an Email Service may be to store and forward outgoing mails, one Function of a Business Process may be to dispatch goods to Customers. • To perform the intended purpose correctly, "The computer is Functioning"
Functional Escalation	**(Service Operation)** Transferring an Incident, Problem or Change to a technical team with a higher level of expertise to assist in an Escalation.
Gap Analysis	**(Continual Service Improvement)** An Activity which compares two sets of data and identifies the differences. Gap Analysis is commonly used to compare a set of Requirements with actual delivery. See Benchmarking.
Governance	Ensuring that Policies and Strategy are actually implemented, and that required Processes are correctly followed. Governance includes defining Roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.
Gradual Recovery	**(Service Design)** A Recovery Option which is also known as Cold Standby. Provision is made to Recover the IT Service in a period of time greater than 72 hours. Gradual Recovery typically uses a Portable or Fixed Facility that has environmental support and network cabling, but no computer Systems. The hardware and software are installed as part of the IT Service Continuity Plan.
Guideline	A Document describing Best Practice, that recommends what should be done. Compliance to a guideline is not normally enforced. See Standard.
Help Desk	**(Service Operation)** A point of contact for Users to log Incidents. A Help Desk is usually more technically focussed than a Service Desk and does not provide a Single Point of Contact for all interaction. The term Help Desk is often used as a synonym for Service Desk.
Hierarchic Escalation	**(Service Operation)** Informing or involving more senior levels of management to assist in an Escalation.
High Availability	**(Service Design)** An approach or Design that minimises or hides the effects of Configuration Item Failure on the Users of an IT Service. High Availability solutions are Designed to achieve an agreed level of Availability and make use of techniques such as Fault Tolerance, Resilience and fast Recovery to reduce the number of Incidents, and the Impact of Incidents.
Hot Standby	Synonym for Fast Recovery or Immediate Recovery.
Identity	**(Service Operation)** A unique name that is used to identify a User, person or Role. The Identity is used to grant Rights to that User, person, or Role. Example identities might be the username SmithJ or the Role "Change manager".
Immediate	**(Service Design)** A Recovery Option which is also known as Hot Standby.

Term	Definition
Recovery	Provision is made to Recover the IT Service with no loss of Service. Immediate Recovery typically uses mirroring, load balancing and split site technologies.
Impact	**(Service Operation) (Service Transition)** A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.
Incident	**(Service Operation)** An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident. For example Failure of one disk from a mirror set.
Incident Management	**(Service Operation)** The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible.
Incident Record	**(Service Operation)** A Record containing the details of an Incident. Each Incident record documents the Lifecycle of a single Incident.
Indirect Cost	**(Service Strategy)** A Cost of providing an IT Service which cannot be allocated in full to a specific Customer. For example Cost of providing shared Servers or software licenses. Also known as Overhead. See Direct Cost.
Information Security Management (ISM)	**(Service Design)** The Process that ensures the Confidentiality, Integrity and Availability of an Organisation's Assets, information, data and IT Services. Information Security Management usually forms part of an Organisational approach to Security Management which has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls etc., for the entire Organisation.
Information Security Management System (ISMS)	**(Service Design)** The framework of Policy, Processes, Standards, Guidelines and tools that ensures an Organisation can achieve its Information Security Management Objectives.
Information Security Policy	**(Service Design)** The Policy that governs the Organisation's approach to Information Security Management.
Information Technology (IT)	The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.
Infrastructure Service	An IT Service that is not directly used by the Business, but is required by the IT Service Provider so they can provide other IT Services. For example Directory Services, naming services, or communication services.
Insourcing	Synonym for Internal Sourcing.
Integrity	**(Service Design)** A security principle that ensures data and Configuration Items are only modified by authorised personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events, and human intervention.

Term	Definition
Interactive Voice Response (IVR)	**(Service Operation)** A form of Automatic Call Distribution that accepts User input, such as key presses and spoken commands, to identify the correct destination for incoming Calls.
Intermediate Recovery	**(Service Design)** A Recovery Option which is also known as Warm Standby. Provision is made to Recover the IT Service in a period of time between 24 and 72 hours. Intermediate Recovery typically uses a shared Portable or Fixed Facility that has computer Systems and network Components. The hardware and software will need to be configured, and data will need to be restored, as part of the IT Service Continuity Plan.
Internal Customer	A Customer who works for the same Business as the IT Service Provider. See Internal Service Provider, External Customer.
Internal Metric	A Metric that is used within the IT Service Provider to Monitor the Efficiency, Effectiveness or Cost Effectiveness of the IT Service Provider's internal Processes. Internal Metrics are not normally reported to the Customer of the IT Service. See External Metric.
Internal Rate of Return (IRR)	**(Service Strategy)** A technique used to help make decisions about Capital Expenditure. IRR calculates a figure that allows two or more alternative investments to be compared. A larger IRR indicates a better investment. See Net Present Value, Return on Investment.
Internal Service Provider	**(Service Strategy)** An IT Service Provider which is part of the same Organisation as their Customer. An IT Service Provider may have both Internal Customers and External Customers. See Type I Service Provider, Type II Service Provider, Insource.
Internal Sourcing	**(Service Strategy)** Using an Internal Service Provider to manage IT Services. See Service Sourcing, Type I Service Provider, Type II Service Provider.
International Organization for Standardization (ISO)	The International Organization for Standardization (ISO) is the world's largest developer of Standards. ISO is a non-governmental organization which is a network of the national standards institutes of 156 countries. Further information about ISO is available from http://www.iso.org/
International Standards Organisation	See International Organization for Standardization (ISO)
Internet Service Provider (ISP)	An External Service Provider that provides access to the Internet. Most ISPs also provide other IT Services such as web hosting.
Invocation	**(Service Design)** Initiation of the steps defined in a plan. For example initiating the IT Service Continuity Plan for one or more IT Services.
Ishikawa Diagram	**(Service Operation) (Continual Service Improvement)** A technique that helps a team to identify all the possible causes of a Problem. Originally devised by Kaoru Ishikawa, the output of this technique is a diagram that looks like a fishbone.
ISO 9000	A generic term that refers to a number of international Standards and Guidelines for Quality Management Systems. See http://www.iso.org/ for more information. See ISO.

Term	Definition
ISO 9001	An international Standard for Quality Management Systems. See ISO 9000, Standard.
ISO/IEC 17799	**(Continual Service Improvement)** ISO Code of Practice for Information Security Management. See Standard.
ISO/IEC 20000	ISO Specification and Code of Practice for IT Service Management. ISO/IEC 20000 is aligned with ITIL Best Practice.
ISO/IEC 27001	**(Service Design) (Continual Service Improvement)** ISO Specification for Information Security Management. The corresponding Code of Practice is ISO/IEC 17799. See Standard.
IT Directorate	**(Continual Service Improvement)** Senior Management within a Service Provider, charged with developing and delivering IT services. Most commonly used in UK Government departments.
IT Infrastructure	All of the hardware, software, networks, facilities etc. that are required to Develop, Test, deliver, Monitor, Control or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation.
IT Operations	**(Service Operation)** Activities carried out by IT Operations Control, including Console Management, Job Scheduling, Backup and Restore, and Print and Output Management. IT Operations is also used as a synonym for Service Operation.
IT Operations Control	**(Service Operation)** The Function responsible for Monitoring and Control of the IT Services and IT Infrastructure. See Operations Bridge.
IT Operations Management	**(Service Operation)** The Function within an IT Service Provider which performs the daily Activities needed to manage IT Services and the supporting IT Infrastructure. IT Operations Management includes IT Operations Control and Facilities Management.
IT Service	A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement.
IT Service Continuity Management (ITSCM)	**(Service Design)** The Process responsible for managing Risks that could seriously impact IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels, by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services. ITSCM should be designed to support Business Continuity Management.
IT Service Continuity Plan	**(Service Design)** A Plan defining the steps required to Recover one or more IT Services. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. The IT Service Continuity Plan should be part of a Business Continuity Plan.
IT Service Management	The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service

Term	Definition
(ITSM)	Providers through an appropriate mix of people, Process and Information Technology. See Service Management.
IT Service Management Forum (itSMF)	The IT Service Management Forum is an independent Organisation dedicated to promoting a professional approach to IT Service Management. The itSMF is a not-for-profit membership Organisation with representation in many countries around the world (itSMF Chapters). The itSMF and its membership contribute to the development of ITIL and associated IT Service Management Standards. See http://www.itsmf.com/ for more information.
IT Service Provider	**(Service Strategy)** A Service Provider that provides IT Services to Internal Customers or External Customers.
IT Steering Group (ISG)	A formal group that is responsible for ensuring that Business and IT Service Provider Strategies and Plans are closely aligned. An IT Steering Group includes senior representatives from the Business and the IT Service Provider.
ITIL	A set of Best Practice guidance for IT Service Management. ITIL is owned by the OGC and consists of a series of publications giving guidance on the provision of Quality IT Services, and on the Processes and facilities needed to support them. See http://www.itil.co.uk/ for more information.
Job Description	A Document which defines the Roles, responsibilities, skills and knowledge required by a particular person. One Job Description can include multiple Roles, for example the Roles of Configuration Manager and Change Manager may be carried out by one person.
Job Scheduling	**(Service Operation)** Planning and managing the execution of software tasks that are required as part of an IT Service. Job Scheduling is carried out by IT Operations Management, and is often automated using software tools that run batch or online tasks at specific times of the day, week, month or year.
Kano Model	**(Service Strategy)** A Model developed by Noriaki Kano that is used to help understand Customer preferences. The Kano Model considers Attributes of an IT Service grouped into areas such as Basic Factors, Excitement Factors, Performance Factors etc.
Kepner & Tregoe Analysis	**(Service Operation) (Continual Service Improvement)** A structured approach to Problem solving. The Problem is analysed in terms of what, where, when and extent. Possible causes are identified. The most probable cause is tested. The true cause is verified.
Key Performance Indicator (KPI)	**(Continual Service Improvement)** A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity. KPIs should be selected to ensure that Efficiency, Effectiveness, and Cost Effectiveness are all managed. See Critical Success Factor.
Knowledge Base	**(Service Transition)** A logical database containing the data used by the Service Knowledge Management System.
Knowledge Management	**(Service Transition)** The Process responsible for gathering, analysing, storing and sharing knowledge and information within an Organisation. The primary purpose of Knowledge Management is to improve Efficiency by reducing the

Term	Definition
	need to rediscover knowledge. See Data-to-Information-to-Knowledge-to-Wisdom, Service Knowledge Management System.
Known Error	**(Service Operation)** A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may also be identified by Development or Suppliers.
Known Error Database (KEDB)	**(Service Operation)** A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management. The Known Error Database is part of the Service Knowledge Management System.
Known Error Record	**(Service Operation)** A Record containing the details of a Known Error. Each Known Error Record documents the Lifecycle of a Known Error, including the Status, Root Cause and Workaround. In some implementations a Known Error is documented using additional fields in a Problem Record.
Lifecycle	The various stages in the life of an IT Service, Configuration Item, Incident, Problem, Change etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. For example: • The Lifecycle of an Application includes Requirements, Design, Build, Deploy, Operate, Optimise. • The Expanded Incident Lifecycle includes Detect, Respond, Diagnose, Repair, Recover, Restore. • The lifecycle of a Server may include: Ordered, Received, In Test, Live, Disposed etc.
Line of Service (LOS)	**(Service Strategy)** A Core Service or Supporting Service that has multiple Service Level Packages. A line of Service is managed by a Product Manager and each Service Level Package is designed to support a particular market segment.
Live	**(Service Transition)** Refers to an IT Service or Configuration Item that is being used to deliver Service to a Customer.
Live Environment	**(Service Transition)** A controlled Environment containing Live Configuration Items used to deliver IT Services to Customers.
Maintainability	**(Service Design)** A measure of how quickly and Effectively a Configuration Item or IT Service can be restored to normal working after a Failure. Maintainability is often measured and reported as MTRS. Maintainability is also used in the context of Software or IT Service Development to mean ability to be Changed or Repaired easily.
Major Incident	**(Service Operation)** The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.
Managed Services	**(Service Strategy)** A perspective on IT Services which emphasizes the fact that they are managed. The term Managed Services is also used as a synonym for Outsourced IT Services.
Management	Information that is used to support decision making by managers. Management

Term	Definition
Information	Information is often generated automatically by tools supporting the various IT Service Management Processes. Management Information often includes the values of KPIs such as "Percentage of Changes leading to Incidents", or "first time fix rate".
Management of Risk (MoR)	The OGC methodology for managing Risks. MoR includes all the Activities required to identify and Control the exposure to Risk which may have an impact on the achievement of an Organisation's Business Objectives. See http://www.m-o-r.org/ for more details.
Management System	The framework of Policy, Processes and Functions that ensures an Organisation can achieve its Objectives.
Manual Workaround	A Workaround that requires manual intervention. Manual Workaround is also used as the name of a Recovery Option in which The Business Process Operates without the use of IT Services. This is a temporary measure and is usually combined with another Recovery Option.
Marginal Cost	**(Service Strategy)** The Cost of continuing to provide the IT Service. Marginal Cost does not include investment already made, for example the cost of developing new software and delivering training.
Market Space	**(Service Strategy)** All opportunities that an IT Service Provider could exploit to meet business needs of Customers. The Market Space identifies the possible IT Services that an IT Service Provider may wish to consider delivering.
Maturity	**(Continual Service Improvement)** A measure of the Reliability, Efficiency and Effectiveness of a Process, Function, Organisation etc. The most mature Processes and Functions are formally aligned to Business Objectives and Strategy, and are supported by a framework for continual improvement.
Maturity Level	A named level in a Maturity model such as the Carnegie Mellon Capability Maturity Model Integration.
Mean Time Between Failures (MTBF)	**(Service Design)** A Metric for measuring and reporting Reliability. MTBF is the average time that a Configuration Item or IT Service can perform its agreed Function without interruption. This is measured from when the CI or IT Service starts working, until it next fails.
Mean Time Between Service Incidents (MTBSI)	**(Service Design)** A Metric used for measuring and reporting Reliability. MTBSI is the mean time from when a System or IT Service fails, until it next fails. MTBSI is equal to MTBF + MTRS.
Mean Time To Repair (MTTR)	The average time taken to repair a Configuration Item or IT Service after a Failure. MTTR is measured from when the CI or IT Service fails until it is Repaired. MTTR does not include the time required to Recover or Restore. MTTR is sometimes incorrectly used to mean Mean Time to Restore Service.
Mean Time to Restore Service (MTRS)	The average time taken to Restore a Configuration Item or IT Service after a Failure. MTRS is measured from when the CI or IT Service fails until it is fully Restored and delivering its normal functionality. See Maintainability, Mean Time to Repair.
Metric	**(Continual Service Improvement)** Something that is measured and reported to help manage a Process, IT Service or Activity. See KPI.

Term	Definition
Memorandum of Agreement - SoID	***An Agreement between an IT Service Provider and a Customer, both of whom are State of Idaho Agencies.*** **SoID**
Middleware	**(Service Design)** Software that connects two or more software Components or Applications. Middleware is usually purchased from a Supplier, rather than developed within the IT Service Provider. See Off the Shelf.
Mission Statement	The Mission Statement of an Organisation is a short but complete description of the overall purpose and intentions of that Organisation. It states what is to be achieved, but not how this should be done.
Model	A representation of a System, Process, IT Service, Configuration Item etc. that is used to help understand or predict future behaviour.
Modelling	A technique that is used to predict the future behaviour of a System, Process, IT Service, Configuration Item etc. Modelling is commonly used in Financial Management, Capacity Management and Availability Management.
Monitor Control Loop	**(Service Operation)** Monitoring the output of a Task, Process, IT Service or Configuration Item; comparing this output to a predefined norm; and taking appropriate action based on this comparison.
Monitoring	**(Service Operation)** Repeated observation of a Configuration Item, IT Service or Process to detect Events and to ensure that the current status is known.
Near-Shore	**(Service Strategy)** Provision of Services from a country near the country where the Customer is based. This can be the provision of an IT Service, or of supporting Functions such as Service Desk. See On-shore, Off-shore.
Net Present Value (NPV)	**(Service Strategy)** A technique used to help make decisions about Capital Expenditure. NPV compares cash inflows to cash outflows. Positive NPV indicates that an investment is worthwhile. See Internal Rate of Return, Return on Investment.
Notional Charging	**(Service Strategy)** An approach to Charging for IT Services. Charges to Customers are calculated and Customers are informed of the charge, but no money is actually transferred. Notional Charging is sometimes introduced to ensure that Customers are aware of the Costs they incur, or as a stage during the introduction of real Charging.
Objective	The defined purpose or aim of a Process, an Activity or an Organisation as a whole. Objectives are usually expressed as measurable targets. The term Objective is also informally used to mean a Requirement. See Outcome.
Off the Shelf	Synonym for Commercial Off the Shelf.
Office of Government Commerce (OGC)	OGC owns the ITIL brand (copyright and trademark). OGC is a UK Government department that supports the delivery of the government's procurement agenda through its work in collaborative procurement and in raising levels of procurement skills and capability with departments. It also provides support for complex public sector projects.
Office of Public	OPSI license the Crown Copyright material used in the ITIL publications. They

Term	Definition
Sector Information (OPSI)	are a UK Government department who provide online access to UK legislation, license the re-use of Crown copyright material, manage the Information Fair Trader Scheme, maintain the Government's Information Asset Register and provide advice and guidance on official publishing and Crown copyright.
Off-shore	**(Service Strategy)** Provision of Services from a location outside the country where the Customer is based, often in a different continent. This can be the provision of an IT Service, or of supporting Functions such as Service Desk. See On-shore, Near-shore.
On-shore	**(Service Strategy)** Provision of Services from a location within the country where the Customer is based. See Off-shore, Near-shore.
Operate	To perform as expected. A Process or Configuration Item is said to Operate if it is delivering the Required outputs. Operate also means to perform one or more Operations. For example, to Operate a computer is to do the day-to-day Operations needed for it to perform as expected.
Operation	**(Service Operation)** Day-to-day management of an IT Service, System, or other Configuration Item. Operation is also used to mean any pre-defined Activity or Transaction. For example loading a magnetic tape, accepting money at a point of sale, or reading data from a disk drive.
Operational	The lowest of three levels of Planning and delivery (Strategic, Tactical, Operational). Operational Activities include the day-to-day or short term Planning or delivery of a Business Process or IT Service Management Process. The term Operational is also a synonym for Live.
Operational Cost	Cost resulting from running the IT Services. Often repeating payments. For example staff costs, hardware maintenance and electricity (also known as "current expenditure" or "revenue expenditure"). See Capital Expenditure.
Operational Expenditure (OPEX)	Synonym for Operational Cost.
Operational Level Agreement (OLA)	**(Service Design) (Continual Service Improvement)** An Agreement between an IT Service Provider and another part of the same Organisation. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties. For example there could be an OLA • between the IT Service Provider and a procurement department to obtain hardware in agreed times • between the Service Desk and a Support Group to provide Incident Resolution in agreed times. See Service Level Agreement.
Operations Bridge	**(Service Operation)** A physical location where IT Services and IT Infrastructure are monitored and managed.
Operations Control	Synonym for IT Operations Control.
Operations Management	Synonym for IT Operations Management.

Term	Definition
Opportunity Cost	**(Service Strategy)** A Cost that is used in deciding between investment choices. Opportunity Cost represents the revenue that would have been generated by using the Resources in a different way. For example the Opportunity Cost of purchasing a new Server may include not carrying out a Service Improvement activity that the money could have been spent on. Opportunity cost analysis is used as part of a decision making processes, but is not treated as an actual Cost in any financial statement.
Optimise	Review, Plan and request Changes, in order to obtain the maximum Efficiency and Effectiveness from a Process, Configuration Item, Application etc.
Organisation	A company, legal entity or other institution. Examples of Organisations that are not companies include International Standards Organisation or itSMF. The term Organisation is sometimes used to refer to any entity which has People, Resources and Budgets. For example a Project or Business Unit.
Outcome	The result of carrying out an Activity; following a Process; delivering an IT Service etc. The term Outcome is used to refer to intended results, as well as to actual results. See Objective.
Outsourcing	**(Service Strategy)** Using an External Service Provider to manage IT Services. See Service Sourcing, Type III Service Provider.
Overhead	Synonym for Indirect cost
Pain Value Analysis	**(Service Operation)** A technique used to help identify the Business Impact of one or more Problems. A formula is used to calculate Pain Value based on the number of Users affected, the duration of the Downtime, the Impact on each User, and the cost to the Business (if known).
Pareto Principle	**(Service Operation)** A technique used to prioritise Activities. The Pareto Principle says that 80% of the value of any Activity is created with 20% of the effort. Pareto Analysis is also used in Problem Management to prioritise possible Problem causes for investigation.
Partnership	A relationship between two Organisations which involves working closely together for common goals or mutual benefit. The IT Service Provider should have a Partnership with the Business, and with Third Parties who are critical to the delivery of IT Services. See Value Network.
Passive Monitoring	**(Service Operation)** Monitoring of a Configuration Item, an IT Service or a Process that relies on an Alert or notification to discover the current status. See Active Monitoring.
Pattern of Business Activity (PBA)	**(Service Strategy)** A Workload profile of one or more Business Activities. Patterns of Business Activity are used to help the IT Service Provider understand and plan for different levels of Business Activity. See User Profile.
Percentage utilisation	**(Service Design)** The amount of time that a Component is busy over a given period of time. For example, if a CPU is busy for 1800 seconds in a one hour period, its utilisation is 50%
Performance	A measure of what is achieved or delivered by a System, person, team, Process, or IT Service.

Term	Definition
Performance Anatomy	**(Service Strategy)** An approach to Organisational Culture that integrates, and actively manages, leadership and strategy, people development, technology enablement, performance management and innovation.
Performance Management	**(Continual Service Improvement)** The Process responsible for day-to-day Capacity Management Activities. These include Monitoring, Threshold detection, Performance analysis and Tuning, and implementing Changes related to Performance and Capacity.
Pilot	**(Service Transition)** A limited Deployment of an IT Service, a Release or a Process to the Live Environment. A Pilot is used to reduce Risk and to gain User feedback and Acceptance. See Test, Evaluation.
Plan	A detailed proposal which describes the Activities and Resources needed to achieve an Objective. For example a Plan to implement a new IT Service or Process. ISO/IEC 20000 requires a Plan for the management of each IT Service Management Process.
Plan-Do-Check-Act	**(Continual Service Improvement)** A four stage cycle for Process management, attributed to Edward Deming. Plan-Do-Check-Act is also called the Deming Cycle. PLAN: Design or revise Processes that support the IT Services. DO: Implement the Plan and manage the Processes. CHECK: Measure the Processes and IT Services, compare with Objectives and produce reports ACT: Plan and implement Changes to improve the Processes.
Planned Downtime	**(Service Design)** Agreed time when an IT Service will not be available. Planned Downtime is often used for maintenance, upgrades and testing. See Change Window, Downtime.
Planning	An Activity responsible for creating one or more Plans. For example, Capacity Planning.
PMBOK	A Project management Standard maintained and published by the Project Management Institute. PMBOK stands for Project Management Body of Knowledge. See http://www.pmi.org/ for more information. See PRINCE2.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure etc.
Portable Facility	**(Service Design)** A prefabricated building, or a large vehicle, provided by a Third Party and moved to a site when needed by an IT Service Continuity Plan. See Recovery Option, Fixed Facility.
Post Implementation Review (PIR)	A Review that takes place after a Change or a Project has been implemented. A PIR determines if the Change or Project was successful, and identifies opportunities for improvement.
Practice	A way of working, or a way in which work must be done. Practices can include Activities, Processes, Functions, Standards and Guidelines. See Best Practice.

Term	Definition
Prerequisite for Success (PFS)	An Activity that needs to be completed, or a condition that needs to be met, to enable successful implementation of a Plan or Process. A PFS is often an output from one Process that is a required input to another Process.
Pricing	**(Service Strategy)** The Activity for establishing how much Customers will be Charged.
PRINCE2	The standard UK government methodology for Project management. See http://www.ogc.gov.uk/prince2/ for more information. See PMBOK.
Priority	**(Service Transition) (Service Operation)** A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority2 Incidents must be resolved within 12 hours.
Proactive Monitoring	**(Service Operation)** Monitoring that looks for patterns of Events to predict possible future Failures. See Reactive Monitoring.
Proactive Problem Management	**(Service Operation)** Part of the Problem Management Process. The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management Processes to identify trends or significant Problems.
Problem	**(Service Operation)** A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.
Problem Management	**(Service Operation)** The Process responsible for managing the Lifecycle of all Problems. The primary Objectives of Problem Management are to prevent Incidents from happening, and to minimise the Impact of Incidents that cannot be prevented.
Problem Record	**(Service Operation)** A Record containing the details of a Problem. Each Problem Record documents the Lifecycle of a single Problem.
Procedure	A Document containing steps that specify how to achieve an Activity. Procedures are defined as part of Processes. See Work Instruction.
Process	A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed.
Process Control	The Activity of planning and regulating a Process, with the Objective of performing the Process in an Effective, Efficient, and consistent manner.
Process Manager	A Role responsible for Operational management of a Process. The Process Manager's responsibilities include Planning and co-ordination of all Activities required to carry out, monitor and report on the Process. There may be several Process Managers for one Process, for example regional Change Managers or IT Service Continuity Managers for each data centre. The Process Manager

Term	Definition
	Role is often assigned to the person who carries out the Process Owner Role, but the two Roles may be separate in larger Organisations.
Process Owner	A Role responsible for ensuring that a Process is Fit for Purpose. The Process Owner's responsibilities include sponsorship, Design, Change Management and continual improvement of the Process and its Metrics. This Role is often assigned to the same person who carries out the Process Manager Role, but the two Roles may be separate in larger Organisations.
Production Environment	Synonym for Live Environment.
Profit Centre	**(Service Strategy)** A Business Unit which charges for Services provided. A Profit Centre can be created with the objective of making a profit, recovering Costs, or running at a loss. An IT Service Provider can be run as a Cost Centre or a Profit Centre.
pro-forma	A template, or example Document containing example data that will be replaced with the real values when these are available.
Programme	A number of Projects and Activities that are planned and managed together to achieve an overall set of related Objectives and other Outcomes.
Project	A temporary Organisation, with people and other Assets required to achieve an Objective or other Outcome. Each Project has a Lifecycle that typically includes initiation, Planning, execution, Closure etc. Projects are usually managed using a formal methodology such as PRINCE2.
Projected Service Outage (PSO)	**(Service Transition)** A Document that identifies the effect of planned Changes, maintenance Activities and Test Plans on agreed Service Levels.
PRojects IN Controlled Environments (PRINCE2)	See PRINCE2
Qualification	**(Service Transition)** An Activity that ensures that IT Infrastructure is appropriate, and correctly configured, to support an Application or IT Service. See Validation.
Quality	The ability of a product, Service, or Process to provide the intended value. For example, a hardware Component can be considered to be of high Quality if it performs as expected and delivers the required Reliability. Process Quality also requires an ability to monitor Effectiveness and Efficiency, and to improve them if necessary. See Quality Management System.
Quality Assurance (QA)	**(Service Transition)** The Process responsible for ensuring that the Quality of a product, Service or Process will provide its intended Value.
Quality Management System (QMS)	**(Continual Service Improvement)** The set of Processes responsible for ensuring that all work carried out by an Organisation is of a suitable Quality to reliably meet Business Objectives or Service Levels. See ISO 9000.
Quick Win	**(Continual Service Improvement)** An improvement Activity which is expected

Term	Definition
	to provide a Return on Investment in a short period of time with relatively small Cost and effort. See Pareto Principle.
RACI	**(Service Design) (Continual Service Improvement)** A Model used to help define Roles and Responsibilities. RACI stands for Responsible, Accountable, Consulted and Informed. See Stakeholder.
Reactive Monitoring	**(Service Operation)** Monitoring that takes action in response to an Event. For example submitting a batch job when the previous job completes, or logging an Incident when an Error occurs. See Proactive Monitoring.
Reciprocal Arrangement	**(Service Design)** A Recovery Option. An agreement between two Organisations to share resources in an emergency. For example, Computer Room space or use of a mainframe.
Record	A Document containing the results or other output from a Process or Activity. Records are evidence of the fact that an Activity took place and may be paper or electronic. For example, an Audit report, an Incident Record, or the minutes of a meeting.
Recovery	**(Service Design) (Service Operation)** Returning a Configuration Item or an IT Service to a working state. Recovery of an IT Service often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the IT Service can be made available to the Users (Restoration).
Recovery Option	**(Service Design)** A Strategy for responding to an interruption to Service. Commonly used Strategies are Do Nothing, Manual Workaround, Reciprocal Arrangement, Gradual Recovery, Intermediate Recovery, Fast Recovery, Immediate Recovery. Recovery Options may make use of dedicated facilities, or Third Party facilities shared by multiple Businesses.
Recovery Point Objective (RPO)	**(Service Operation)** The maximum amount of data that may be lost when Service is Restored after an interruption. Recovery Point Objective is expressed as a length of time before the Failure. For example a Recovery Point Objective of one day may be supported by daily Backups, and up to 24 hours of data may be lost. Recovery Point Objectives for each IT Service should be negotiated, agreed and documented, and used as Requirements for Service Design and IT Service Continuity Plans.
Recovery Time Objective (RTO)	**(Service Operation)** The maximum time allowed for recovery of an IT Service following an interruption. The Service Level to be provided may be less than normal Service Level Targets. Recovery Time Objectives for each IT Service should be negotiated, agreed and documented. See Business Impact Analysis.
Redundancy	Synonym for Fault Tolerance. The term Redundant also has a generic meaning of obsolete, or no longer needed.
Relationship	A connection or interaction between two people or things. In Business Relationship Management it is the interaction between the IT Service Provider and the Business. In Configuration Management it is a link between two Configuration Items that identifies a dependency or connection between them.

Term	Definition
	For example Applications may be linked to the Servers they run on, IT Services have many links to all the CIs that contribute to them.
Relationship Processes	The ISO/IEC 20000 Process group that includes Business Relationship Management and Supplier Management.
Release	**(Service Transition)** A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.
Release and Deployment Management	**(Service Transition)** The Process responsible for both Release Management and Deployment.
Release Identification	**(Service Transition)** A naming convention used to uniquely identify a Release. The Release Identification typically includes a reference to the Configuration Item and a version number. For example Microsoft Office 2003 SR2.
Release Management	**(Service Transition)** The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary Objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management is part of the Release and Deployment Management Process.
Release Process	The name used by ISO/IEC 20000 for the Process group that includes Release Management. This group does not include any other Processes. Release Process is also used as a synonym for Release Management Process.
Release Record	**(Service Transition)** A Record in the CMDB that defines the content of a Release. A Release Record has Relationships with all Configuration Items that are affected by the Release.
Release Unit	**(Service Transition)** Components of an IT Service that are normally Released together. A Release Unit typically includes sufficient Components to perform a useful Function. For example one Release Unit could be a Desktop PC, including Hardware, Software, Licenses, Documentation etc. A different Release Unit may be the complete Payroll Application, including IT Operations Procedures and User training.
Release Window	Synonym for Change Window.
Reliability	**(Service Design) (Continual Service Improvement)** A measure of how long a Configuration Item or IT Service can perform its agreed Function without interruption. Usually measured as MTBF or MTBSI. The term Reliability can also be used to state how likely it is that a Process, Function etc. will deliver its required outputs. See Availability.
Remediation	**(Service Transition)** Recovery to a known state after a failed Change or Release.
Repair	**(Service Operation)** The replacement or correction of a failed Configuration Item.
Request for	**(Service Transition)** A formal proposal for a Change to be made. An RFC

Term	Definition
Change (RFC)	includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.
Request Fulfilment	**(Service Operation)** The Process responsible for managing the Lifecycle of all Service Requests.
Requirement	**(Service Design)** A formal statement of what is needed. For example a Service Level Requirement, a Project Requirement or the required Deliverables for a Process. See Statement of Requirements.
Resilience	**(Service Design)** The ability of a Configuration Item or IT Service to resist Failure or to Recover quickly following a Failure. For example, an armoured cable will resist failure when put under stress. See Fault Tolerance.
Resolution	**(Service Operation)** Action taken to repair the Root Cause of an Incident or Problem, or to implement a Workaround. In ISO/IEC 20000, Resolution Processes is the Process group that includes Incident and Problem Management.
Resolution Processes	The ISO/IEC 20000 Process group that includes Incident Management and Problem Management.
Resource	**(Service Strategy)** A generic term that includes IT Infrastructure, people, money or anything else that might help to deliver an IT Service. Resources are considered to be Assets of an Organisation. See Capability, Service Asset.
Response Time	A measure of the time taken to complete an Operation or Transaction. Used in Capacity Management as a measure of IT Infrastructure Performance, and in Incident Management as a measure of the time taken to answer the phone, or to start Diagnosis.
Responsiveness	A measurement of the time taken to respond to something. This could be Response Time of a Transaction, or the speed with which an IT Service Provider responds to an Incident or Request for Change etc.
Restoration of Service	See Restore.
Restore	**(Service Operation)** Taking action to return an IT Service to the Users after Repair and Recovery from an Incident. This is the primary Objective of Incident Management.
Retire	**(Service Transition)** Permanent removal of an IT Service, or other Configuration Item, from the Live Environment. Retired is a stage in the Lifecycle of many Configuration Items.
Return on Investment (ROI)	**(Service Strategy) (Continual Service Improvement)** A measurement of the expected benefit of an investment. In the simplest sense it is the net profit of an investment divided by the net worth of the assets invested. See Net Present Value, Value on Investment.
Return to Normal	**(Service Design)** The phase of an IT Service Continuity Plan during which full normal operations are resumed. For example, if an alternate data centre has

Term	Definition
	been in use, then this phase will bring the primary data centre back into operation, and restore the ability to invoke IT Service Continuity Plans again.
Review	An evaluation of a Change, Problem, Process, Project etc. Reviews are typically carried out at predefined points in the Lifecycle, and especially after Closure. The purpose of a Review is to ensure that all Deliverables have been provided, and to identify opportunities for improvement. See Post Implementation Review.
Rights	**(Service Operation)** Entitlements, or permissions, granted to a User or Role. For example the Right to modify particular data, or to authorize a Change.
Risk	A possible Event that could cause harm or loss, or affect the ability to achieve Objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the Impact it would have if it occurred.
Risk Assessment	The initial steps of Risk Management. Analysing the value of Assets to the business, identifying Threats to those Assets, and evaluating how Vulnerable each Asset is to those Threats. Risk Assessment can be quantitative (based on numerical data) or qualitative.
Risk Management	The Process responsible for identifying, assessing and controlling Risks. See Risk Assessment.
Role	A set of responsibilities, Activities and authorities granted to a person or team. A Role is defined in a Process. One person or team may have multiple Roles, for example the Roles of Configuration Manager and Change Manager may be carried out by a single person.
Rollout	**(Service Transition)** Synonym for Deployment. Most often used to refer to complex or phased Deployments or Deployments to multiple locations.
Root Cause	**(Service Operation)** The underlying or original cause of an Incident or Problem.
Root Cause Analysis (RCA)	**(Service Operation)** An Activity that identifies the Root Cause of an Incident or Problem. RCA typically concentrates on IT Infrastructure failures. See Service Failure Analysis.
Running Costs	Synonym for Operational Costs
Scalability	The ability of an IT Service, Process, Configuration Item etc. to perform its agreed Function when the Workload or Scope changes.
Scope	The boundary, or extent, to which a Process, Procedure, Certification, Contract etc. applies. For example the Scope of Change Management may include all Live IT Services and related Configuration Items, the Scope of an ISO/IEC 20000 Certificate may include all IT Services delivered out of a named data centre.
Second-line Support	**(Service Operation)** The second level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other Resources.
Security	See Information Security Management
Security Management	Synonym for Information Security Management

Term	Definition
Security Policy	Synonym for Information Security Policy
Separation of Concerns (SoC)	**(Service Strategy)** An approach to Designing a solution or IT Service that divides the problem into pieces that can be solved independently. This approach separates "what" is to be done from "how" it is to be done.
Server	**(Service Operation)** A computer that is connected to a network and provides software Functions that are used by other computers.
Service	A means of delivering value to Customers by facilitating Outcomes Customers want to achieve without the ownership of specific Costs and Risks.
Service Acceptance Criteria (SAC)	**(Service Transition)** A set of criteria used to ensure that an IT Service meets its functionality and Quality Requirements and that the IT Service Provider is ready to Operate the new IT Service when it has been Deployed. See Acceptance.
Service Analytics	**(Service Strategy)** A technique used in the Assessment of the Business Impact of Incidents. Service Analytics Models the dependencies between Configuration Items, and the dependencies of IT Services on Configuration Items.
Service Asset	Any Capability or Resource of a Service Provider. See Asset.
Service Asset and Configuration Management (SACM)	**(Service Transition)** The Process responsible for both Configuration Management and Asset Management.
Service Capacity Management (SCM)	**(Service Design) (Continual Service Improvement)** The Activity responsible for understanding the Performance and Capacity of IT Services. The Resources used by each IT Service and the pattern of usage over time are collected, recorded, and analysed for use in the Capacity Plan. See Business Capacity Management, Component Capacity Management.
Service Catalogue	**(Service Design)** A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes. See Contract Portfolio.
Service Continuity Management	Synonym for IT Service Continuity Management.
Service Contract	**(Service Strategy)** A Contract to deliver one or more IT Services. The term Service Contract is also used to mean any Agreement to deliver IT Services, whether this is a legal Contract or an SLA. See Contract Portfolio.
Service Culture	A Customer oriented Culture. The major Objectives of a Service Culture are Customer satisfaction and helping the Customer to achieve their Business Objectives.

Term	Definition
Service Design	**(Service Design)** A stage in the Lifecycle of an IT Service. Service Design includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See Design.
Service Design Package	**(Service Design)** Document(s) defining all aspects of an IT Service and its Requirements through each stage of its Lifecycle. A Service Design Package is produced for each new IT Service, major Change, or IT Service Retirement.
Service Desk	**(Service Operation)** The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.
Service Failure Analysis (SFA)	**(Service Design)** An Activity that identifies underlying causes of one or more IT Service interruptions. SFA identifies opportunities to improve the IT Service Provider's Processes and tools, and not just the IT Infrastructure. SFA is a time constrained, project-like activity, rather than an ongoing process of analysis. See Root Cause Analysis.
Service Hours	**(Service Design) (Continual Service Improvement)** An agreed time period when a particular IT Service should be Available. For example, "Monday-Friday 08:00 to 17:00 except public holidays". Service Hours should be defined in a Service Level Agreement.
Service Improvement Plan (SIP)	**(Continual Service Improvement)** A formal Plan to implement improvements to a Process or IT Service.
Service Knowledge Management System (SKMS)	**(Service Transition)** A set of tools and databases that are used to manage knowledge and information. The SKMS includes the Configuration Management System, as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT Service Provider needs to manage the full Lifecycle of IT Services.
Service Level	Measured and reported achievement against one or more Service Level Targets. The term Service Level is sometimes used informally to mean Service Level Target.
Service Level Agreement (SLA)	**(Service Design) (Continual Service Improvement)** An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers. See Operational Level Agreement. ***SoID – For the State of Idaho, the Agreement will be in the form of a Memorandum of Agreement (MOA).***
Service Level Management (SLM)	**(Service Design) (Continual Service Improvement)** The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.
Service Level Package (SLP)	**(Service Strategy)** A defined level of Utility and Warranty for a particular Service Package. Each SLP is designed to meet the needs of a particular

Term	Definition
	Pattern of Business Activity. See Line of Service.
Service Level Requirement (SLR)	**(Service Design) (Continual Service Improvement)** A Customer Requirement for an aspect of an IT Service. SLRs are based on Business Objectives and are used to negotiate agreed Service Level Targets.
Service Level Target	**(Service Design) (Continual Service Improvement)** A commitment that is documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements, and are needed to ensure that the IT Service design is Fit for Purpose. Service Level Targets should be SMART, and are usually based on KPIs.
Service Maintenance Objective	**(Service Operation)** The expected time that a Configuration Item will be unavailable due to planned maintenance Activity.
Service Management	Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.
Service Management Lifecycle	An approach to IT Service Management that emphasizes the importance of coordination and Control across the various Functions, Processes, and Systems necessary to manage the full Lifecycle of IT Services. The Service Management Lifecycle approach considers the Strategy, Design, Transition, Operation and Continuous Improvement of IT Services.
Service Manager	A manager who is responsible for managing the end-to-end Lifecycle of one or more IT Services. The term Service Manager is also used to mean any manager within the IT Service Provider. Most commonly used to refer to a Business Relationship Manager, a Process Manager, an Account Manager or a senior manager with responsibility for IT Services overall.
Service Operation	**(Service Operation)** A stage in the Lifecycle of an IT Service. Service Operation includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See Operation.
Service Owner	**(Continual Service Improvement)** A Role which is accountable for the delivery of a specific IT Service.
Service Package	**(Service Strategy)** A detailed description of an IT Service that is available to be delivered to Customers. A Service Package includes a Service Level Package and one or more Core Services and Supporting Services.
Service Pipeline	**(Service Strategy)** A database or structured Document listing all IT Services that are under consideration or Development, but are not yet available to Customers. The Service Pipeline provides a Business view of possible future IT Services and is part of the Service Portfolio which is not normally published to Customers.
Service Portfolio	**(Service Strategy)** The complete set of Services that are managed by a Service Provider. The Service Portfolio is used to manage the entire Lifecycle of all Services, and includes three Categories: Service Pipeline (proposed or in Development); Service Catalogue (Live or available for Deployment); and Retired Services. See Service Portfolio Management, Contract Portfolio.

Term	Definition
Service Portfolio Management (SPM)	**(Service Strategy)** The Process responsible for managing the Service Portfolio. Service Portfolio Management considers Services in terms of the Business value that they provide.
Service Potential	**(Service Strategy)** The total possible value of the overall Capabilities and Resources of the IT Service Provider.
Service Provider	**(Service Strategy)** An Organisation supplying Services to one or more Internal Customers or External Customers. Service Provider is often used as an abbreviation for IT Service Provider. See Type I Service Provider, Type II Service Provider, Type III Service Provider.
Service Provider Interface (SPI)	**(Service Strategy)** An interface between the IT Service Provider and a User, Customer, Business Process, or a Supplier. Analysis of Service Provider Interfaces helps to coordinate end-to-end management of IT Services.
Service Provisioning Optimization (SPO)	**(Service Strategy)** Analysing the finances and constraints of an IT Service to decide if alternative approaches to Service delivery might reduce Costs or improve Quality.
Service Reporting	**(Continual Service Improvement)** The Process responsible for producing and delivering reports of achievement and trends against Service Levels. Service Reporting should agree the format, content and frequency of reports with Customers.
Service Request	**(Service Operation)** A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted. See Request Fulfilment.
Service Sourcing	**(Service Strategy)** The Strategy and approach for deciding whether to provide a Service internally or to Outsource it to an External Service Provider. Service Sourcing also means the execution of this Strategy. Service Sourcing includes: • Internal Sourcing - Internal or Shared Services using Type I or Type II Service Providers. • Traditional Sourcing - Full Service Outsourcing using a Type III Service Provider. • Multivendor Sourcing - Prime, Consortium or Selective Outsourcing using Type III Service Providers.
Service Strategy	**(Service Strategy)** The title of one of the Core ITIL publications. Service Strategy establishes an overall Strategy for IT Services and for IT Service Management.
Service Transition	**(Service Transition)** A stage in the Lifecycle of an IT Service. Service Transition includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See Transition.
Service Utility	**(Service Strategy)** The Functionality of an IT Service from the Customer's perspective. The Business value of an IT Service is created by the combination of Service Utility (what the Service does) and Service Warranty (how well it does

Term	Definition
	it). See Utility.
Service Validation and Testing	**(Service Transition)** The Process responsible for Validation and Testing of a new or Changed IT Service. Service Validation and Testing ensures that the IT Service matches its Design Specification and will meet the needs of the Business.
Service Valuation	**(Service Strategy)** A measurement of the total Cost of delivering an IT Service, and the total value to the Business of that IT Service. Service Valuation is used to help the Business and the IT Service Provider agree on the value of the IT Service.
Service Warranty	**(Service Strategy)** Assurance that an IT Service will meet agreed Requirements. This may be a formal Agreement such as a Service Level Agreement or Contract, or may be a marketing message or brand image. The Business value of an IT Service is created by the combination of Service Utility (what the Service does) and Service Warranty (how well it does it). See Warranty.
Serviceability	**(Service Design) (Continual Service Improvement)** The ability of a Third Party Supplier to meet the terms of their Contract. This Contract will include agreed levels of Reliability, Maintainability or Availability for a Configuration Item.
Shift	**(Service Operation)** A group or team of people who carry out a specific Role for a fixed period of time. For example there could be four shifts of IT Operations Control personnel to support an IT Service that is used 24 hours a day.
Simulation modelling	**(Service Design) (Continual Service Improvement)** A technique that creates a detailed Model to predict the behaviour of a Configuration Item or IT Service. Simulation Models can be very accurate but are expensive and time consuming to create. A Simulation Model is often created by using the actual Configuration Items that are being modelled, with artificial Workloads or Transactions. They are used in Capacity Management when accurate results are important. A simulation model is sometimes called a Performance Benchmark.
Single Point of Contact	**(Service Operation)** Providing a single consistent way to communicate with an Organisation or Business Unit. For example, a Single Point of Contact for an IT Service Provider is usually called a Service Desk.
Single Point of Failure (SPOF)	**(Service Design)** Any Configuration Item that can cause an Incident when it fails, and for which a Countermeasure has not been implemented. A SPOF may be a person, or a step in a Process or Activity, as well as a Component of the IT Infrastructure. See Failure.
SLAM Chart	**(Continual Service Improvement)** A Service Level Agreement Monitoring Chart is used to help monitor and report achievements against Service Level Targets. A SLAM Chart is typically colour coded to show whether each agreed Service Level Target has been met, missed, or nearly missed during each of the previous 12 months.
SMART	**(Service Design) (Continual Service Improvement)** An acronym for helping to remember that targets in Service Level Agreements and Project Plans should be Specific, Measurable, Achievable, Relevant and Timely.

Term	Definition
Snapshot	**(Service Transition)** The current state of a Configuration as captured by a discovery tool. Also used as a synonym for Benchmark. See Baseline.
Source	See Service Sourcing.
Specification	A formal definition of Requirements. A Specification may be used to define technical or Operational Requirements, and may be internal or external. Many public Standards consist of a Code of Practice and a Specification. The Specification defines the Standard against which an Organisation can be Audited.
Stakeholder	All people who have an interest in an Organisation, Project, IT Service etc. Stakeholders may be interested in the Activities, targets, Resources, or Deliverables. Stakeholders may include Customers, Partners, employees, shareholders, owners, etc. See RACI.
Standard	A mandatory Requirement. Examples include ISO/IEC 20000 (an international Standard), an internal security Standard for Unix configuration, or a government Standard for how financial Records should be maintained. The term Standard is also used to refer to a Code of Practice or Specification published by a Standards Organisation such as ISO or BSI. See Guideline.
Standard Change	**(Service Transition)** A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request. See Change Model.
Standard Operating Procedures (SOP)	**(Service Operation)** Procedures used by IT Operations Management.
Standby	**(Service Design)** Used to refer to Resources that are not required to deliver the Live IT Services, but are available to support IT Service Continuity Plans. For example a Standby data centre may be maintained to support Hot Standby, Warm Standby or Cold Standby arrangements.
Statement of requirements (SOR)	**(Service Design)** A Document containing all Requirements for a product purchase, or a new or changed IT Service. See Terms of Reference.
Status	The name of a required field in many types of Record. It shows the current stage in the Lifecycle of the associated Configuration Item, Incident, Problem etc.
Status Accounting	**(Service Transition)** The Activity responsible for recording and reporting the Lifecycle of each Configuration Item.
Storage Management	**(Service Operation)** The Process responsible for managing the storage and maintenance of data throughout its Lifecycle.
Strategic	**(Service Strategy)** The highest of three levels of Planning and delivery (Strategic, Tactical, Operational). Strategic Activities include Objective setting

Term	Definition
	and long term Planning to achieve the overall Vision.
Strategy	**(Service Strategy)** A Strategic Plan designed to achieve defined Objectives.
Super User	**(Service Operation)** A User who helps other Users, and assists in communication with the Service Desk or other parts of the IT Service Provider. Super Users typically provide support for minor Incidents and training.
Supplier	**(Service Strategy) (Service Design)** A Third Party responsible for supplying goods or Services that are required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and Outsourcing Organisations. See Underpinning Contract, Supply Chain.
Supplier and Contract Database (SCD)	**(Service Design)** A database or structured Document used to manage Supplier Contracts throughout their Lifecycle. The SCD contains key Attributes of all Contracts with Suppliers, and should be part of the Service Knowledge Management System.
Supplier Management	**(Service Design)** The Process responsible for ensuring that all Contracts with Suppliers support the needs of the Business, and that all Suppliers meet their contractual commitments.
Supply Chain	**(Service Strategy)** The Activities in a Value Chain carried out by Suppliers. A Supply Chain typically involves multiple Suppliers, each adding value to the product or Service. See Value Network.
Support Group	**(Service Operation)** A group of people with technical skills. Support Groups provide the Technical Support needed by all of the IT Service Management Processes. See Technical Management.
Support Hours	**(Service Design) (Service Operation)** The times or hours when support is available to the Users. Typically this is the hours when the Service Desk is available. Support Hours should be defined in a Service Level Agreement, and may be different from Service Hours. For example, Service Hours may be 24 hours a day, but the Support Hours may be 07:00 to 19:00.
Supporting Service	**(Service Strategy)** A Service that enables or enhances a Core Service. For example a Directory Service or a Backup Service. See Service Package.
SWOT Analysis	**(Continual Service Improvement)** A technique that reviews and analyses the internal strengths and weaknesses of an Organisation and the external opportunities and threats which it faces SWOT stands for Strengths, Weaknesses, Opportunities and Threats.
System	A number of related things that work together to achieve an overall Objective. For example: • A computer System including hardware, software and Applications. • A management System, including multiple Processes that are planned and managed together. For example a Quality Management System. • A Database Management System or Operating System that includes many software modules that are designed to perform a set of related Functions.

Term	Definition
System Management	The part of IT Service Management that focuses on the management of IT Infrastructure rather than Process.
Tactical	The middle of three levels of Planning and delivery (Strategic, Tactical, Operational). Tactical Activities include the medium term Plans required to achieve specific Objectives, typically over a period of weeks to months.
Tag	**(Service Strategy)** A short code used to identify a Category. For example tags EC1, EC2, EC3 etc. might be used to identify different Customer outcomes when analysing and comparing Strategies. The term Tag is also used to refer to the Activity of assigning Tags to things.
Technical Management	**(Service Operation)** The Function responsible for providing technical skills in support of IT Services and management of the IT Infrastructure. Technical Management defines the Roles of Support Groups, as well as the tools, Processes and Procedures required.
Technical Observation (TO)	**(Continual Service Improvement)** A technique used in Service Improvement, Problem investigation and Availability Management. Technical support staff meet to monitor the behaviour and Performance of an IT Service and make recommendations for improvement.
Technical Service	Synonym for Infrastructure Service.
Technical Support	Synonym for Technical Management.
Tension Metrics	**(Continual Service Improvement)** A set of related Metrics, in which improvements to one Metric have a negative effect on another. Tension Metrics are designed to ensure that an appropriate balance is achieved.
Terms of Reference (TOR)	**(Service Design)** A Document specifying the Requirements, Scope, Deliverables, Resources and schedule for a Project or Activity.
Test	**(Service Transition)** An Activity that verifies that a Configuration Item, IT Service, Process, etc. meets its Specification or agreed Requirements. See Service Validation and Testing, Acceptance.
Test Environment	**(Service Transition)** A controlled Environment used to Test Configuration Items, Builds, IT Services, Processes etc.
Third Party	A person, group, or Business who is not part of the Service Level Agreement for an IT Service, but is required to ensure successful delivery of that IT Service. For example a software Supplier, a hardware maintenance company, or a facilities department. Requirements for Third Parties are typically specified in Underpinning Contracts or Operational Level Agreements.
Third-line Support	**(Service Operation)** The third level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other Resources.
Threat	Anything that might exploit a Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example a fire is a Threat that could exploit the Vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management, but also applies to other areas such as Problem and Availability

Term	Definition
	Management.
Threshold	The value of a Metric which should cause an Alert to be generated, or management action to be taken. For example "Priority1 Incident not solved within 4 hours", "more than 5 soft disk errors in an hour", or "more than 10 failed changes in a month".
Throughput	**(Service Design)** A measure of the number of Transactions, or other Operations, performed in a fixed time. For example 5000 emails sent per hour, or 200 disk I/Os per second.
Total Cost of Ownership (TCO)	**(Service Strategy)** A methodology used to help make investment decisions. TCO assesses the full Lifecycle Cost of owning a Configuration Item, not just the initial Cost or purchase price. See Total Cost of Utilization.
Total Cost of Utilization (TCU)	**(Service Strategy)** A methodology used to help make investment and Service Sourcing decisions. TCU assesses the full Lifecycle Cost to the Customer of using an IT Service. See Total Cost of Ownership.
Total Quality Management (TQM)	**(Continual Service Improvement)** A methodology for managing continual Improvement by using a Quality Management System. TQM establishes a Culture involving all people in the Organisation in a Process of continual monitoring and improvement.
Transaction	A discrete Function performed by an IT Service. For example transferring money from one bank account to another. A single Transaction may involve numerous additions, deletions and modifications of data. Either all of these complete successfully or none of them is carried out.
Transition	**(Service Transition)** A change in state, corresponding to a movement of an IT Service or other Configuration Item from one Lifecycle status to the next.
Transition Planning and Support	**(Service Transition)** The Process responsible for Planning all Service Transition Processes and co-ordinating the resources that they require. These Service Transition Processes are Change Management, Service Asset and Configuration Management, Release and Deployment Management, Service Validation and Testing, Evaluation, and Knowledge Management.
Trend Analysis	**(Continual Service Improvement)** Analysis of data to identify time related patterns. Trend Analysis is used in Problem Management to identify common Failures or fragile Configuration Items, and in Capacity Management as a Modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.
Tuning	The Activity responsible for Planning Changes to make the most efficient use of Resources. Tuning is part of Performance Management, which also includes Performance Monitoring and implementation of the required Changes.
Type I Service Provider	**(Service Strategy)** An Internal Service Provider that is embedded within a Business Unit. There may be several Type I Service Providers within an Organisation.
Type II Service Provider	**(Service Strategy)** An Internal Service Provider that provides shared IT Services to more than one Business Unit.

Term	Definition
Type III Service Provider	**(Service Strategy)** A Service Provider that provides IT Services to External Customers.
Underpinning Contract (UC)	**(Service Design)** A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.
Unit Cost	**(Service Strategy)** The Cost to the IT Service Provider of providing a single Component of an IT Service. For example the Cost of a single desktop PC, or of a single Transaction.
Urgency	**(Service Transition) (Service Design)** A measure of how long it will be until an Incident, Problem or Change has a significant Impact on the Business. For example a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the financial year. Impact and Urgency are used to assign Priority.
Usability	**(Service Design)** The ease with which an Application, product, or IT Service can be used. Usability Requirements are often included in a Statement of Requirements.
Use Case	**(Service Design)** A technique used to define required functionality and Objectives, and to Design Tests. Use Cases define realistic scenarios that describe interactions between Users and an IT Service or other System. See Change Case.
User	A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.
User Profile (UP)	**(Service Strategy)** A pattern of User demand for IT Services. Each User Profile includes one or more Patterns of Business Activity.
Utility	**(Service Strategy)** Functionality offered by a Product or Service to meet a particular need. Utility is often summarised as "what it does". See Service Utility.
Validation	**(Service Transition)** An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable meets the needs of the Business. Validation ensures that Business Requirements are met even though these may have changed since the original Design. See Verification, Acceptance, Qualification, Service Validation and Testing.
Value Chain	**(Service Strategy)** A sequence of Processes that creates a product or Service that is of value to a Customer. Each step of the sequence builds on the previous steps and contributes to the overall product or Service. See Value Network.
Value for Money	An informal measure of Cost Effectiveness. Value for Money is often based on a comparison with the Cost of alternatives. See Cost Benefit Analysis.
Value Network	**(Service Strategy)** A complex set of Relationships between two or more groups or organisations. Value is generated through exchange of knowledge, information, goods or Services. See Value Chain, Partnership.

Term	Definition
Value on Investment (VOI)	**(Continual Service Improvement)** A measurement of the expected benefit of an investment. VOI considers both financial and intangible benefits. See Return on Investment.
Variable Cost	**(Service Strategy)** A Cost that depends on how much the IT Service is used, how many products are produced, the number and type of Users, or something else that cannot be fixed in advance. See Variable Cost Dynamics.
Variable Cost Dynamics	**(Service Strategy)** A technique used to understand how overall Costs are impacted by the many complex variable elements that contribute to the provision of IT Services.
Variance	The difference between a planned value and the actual measured value. Commonly used in Financial Management, Capacity Management and Service Level Management, but could apply in any area where Plans are in place.
Verification	**(Service Transition)** An Activity that ensures a new or changed IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and matches its Design Specification. See Validation, Acceptance, Service Validation and Testing.
Verification and Audit	**(Service Transition)** The Activities responsible for ensuring that information in the CMDB is accurate and that all Configuration Items have been identified and recorded in the CMDB. Verification includes routine checks that are part of other Processes. For example, verifying the serial number of a desktop PC when a User logs an Incident. Audit is a periodic, formal check.
Version	**(Service Transition)** A Version is used to identify a specific Baseline of a Configuration Item. Versions typically use a naming convention that enables the sequence or date of each Baseline to be identified. For example Payroll Application Version 3 contains updated functionality from Version 2.
Vision	A description of what the Organisation intends to become in the future. A Vision is created by senior management and is used to help influence Culture and Strategic Planning.
Vital Business Function (VBF)	**(Service Design)** A Function of a Business Process which is critical to the success of the Business. Vital Business Functions are an important consideration of Business Continuity Management, IT Service Continuity Management and Availability Management.
Vulnerability	A weakness that could be exploited by a Threat. For example an open firewall port, a password that is never changed, or a flammable carpet. A missing Control is also considered to be a Vulnerability.
Warm Standby	Synonym for Intermediate Recovery.
Warranty	**(Service Strategy)** A promise or guarantee that a product or Service will meet its agreed Requirements. See Service Validation and Testing, Service Warranty.
Work in Progress (WIP)	A Status that means Activities have started but are not yet complete. It is commonly used as a Status for Incidents, Problems, Changes etc.
Work Instruction	A Document containing detailed instructions that specify exactly what steps to follow to carry out an Activity. A Work Instruction contains much more detail than

Term	Definition
	a Procedure and is only created if very detailed instructions are needed.
Workaround	**(Service Operation)** Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.
Workload	The Resources required to deliver an identifiable part of an IT Service. Workloads may be Categorised by Users, groups of Users, or Functions within the IT Service. This is used to assist in analysing and managing the Capacity, Performance and Utilisation of Configuration Items and IT Services. The term Workload is sometimes used as a synonym for Throughput.

Appendix D: Release Plan Template

Release Plan

<project name>

<author organization>
(date)
Version <n.n>
Boise, Idaho

DOCUMENT REVISION HISTORY:

Version	Author	Comments	Date
<n.n>	<author name>	<any related notes or comments>	<revision date>

Table of Contents

Description 1
Purpose 1
Context 1
1.0 Release Plan Overview 2
1.1 Release Implementation Schedule 2
1.2 Release Strategy 2
1.3 Rollback Strategy 2
2.0 Risk Plan 3
2.1 Risks 3
2.2 Risk Mitigation Strategy 3
3.0 Support Plan 4
3.1 Staffing Schedule 4
3.2 Required Resources 4
3.3 Production Operations Activities 4
4.0 Communication Plan 5
4.1 Communication Plan 5
4.2 Communication Plan Scope 5
4.3 Communication Content 5
4.4 Communication Methods and Tools 6
4.5 Communication Schedule 6
5.0 Test Plan 7
5.1 Test Plan 7
5.2 Scope of Test Plan 7
5.3 Tracking of Testing 7
6.0 Training Plan 8
6.1 Training Plan 8
6.2 Scope of Training Plan 8
6.3 Training Program Description 9
6.4 Training Schedule 9
7.0 Finish / Closing Plan 10
7.1 Document the Release 10
7.2 Track and Resolve Issues 10
7.3 Close 10
8.0 Representative Release Implementation Schedule 11
9.0 Representative Risk Log 12
10.0 Representative Test Plan 13
11.0 Representative Test Case 14
12.0 Representative Traceability Matrix 15
13.0 Representative Support Plan 16

Description

The release plan documents the plan and strategy associated with a specific release, and all of the associated activities with the release.

Purpose

The primary purpose of the document is to improve and share communications across all of the parties affected by the release.

Context

The Release Plan template is part of the Change Management process. The Major Release Manager creates this document, following development of the release strategy. This plan should be tailored to fit the release requirements to the plan.

1. Release Plan Overview

Overall strategy detailed describing what business objectives will be achieved in as time-effective a manner as possible.

Overview and general outline of activities presenting each of the aspects of the activities to be performed: communication, staffing, setting up of monitoring/controls, acceptance testing, and training.

Description of the types of changes covered by each release.

List of organizational entities affected by the releases.

Statement of the release plan objectives in terms of business results to be achieved.

Statement of the main priorities, constraints, and standards to be followed if modifications need to be made to the initial plan.

[Enter content here]

1.1. Release Implementation Schedule

Scheduling of the activities of all the aspects covering the releases and the forecast implementation timeframes:

- ***Duration of activities and start and end dates of each;***
- ***Activity dependencies (what must happen first, second, third...);***
- ***Participant groups concerned (client groups, external participants, and change agents);***
- ***Presentation of the schedule of activities through one or more diagrams (Gantt or other type).***

An example Release Implementation Schedule outline is provided at the end of this template.

[Enter content here]

1.2. Release Strategy

Determine the type of release that will minimize risk and still meet your requirements. Typical release strategies are Big Bang or Phased. Big Bang normally means you will do one release and implement your change all at the same time. A phased approach will normally reduce risk and impact of failure, but could make the release more complex and take more time. There are other release strategies:

- ***Release strategy;***
- ***Rational;***

[Enter content here]

1.3. Rollback Strategy

A rollback strategy is normally required as part of change management, but if rollback has not been considered, it should be as part of the release. Consider impact of failure, time needed to rollback, and complexity of rollback. Schedule the release with rollback requirements in mind;

- ***Rollback strategy;***
- ***Rational;***

1.4. [Enter content here]

2. Risk Plan

2.1. Risks

Identify risks associated with the release:

- ***List known risks;***
- ***Use brainstorming with others to identify risks;***
- ***Review lessons learned from previous releases to identify risks;***
-
- ***An example Risk Log is provided at the end of this template.***

[Enter content here]

2.2. Risk Mitigation Strategy

Find ways to manage each risk;

[Enter content here]

3. Support Plan

3.1. Staffing Schedule

Presentation of the schedule of staffing activities listing:

- ***The logical sequencing of the staffing activities;***
- ***The duration of these activities and the dates on which they will take place;***
- ***The participant groups concerned (client groups and change agents);***
- ***The pivotal dates marking, in particular, synchronization with other plans such as installation plans, training plans, communication plans, etc.***

[Enter content here]

3.2. Required Resources

Qualification and quantity of human and material resources required for staffing activities.

[Enter content here]

3.3. Production Operations Activities

Description of:

- ***Installation of control procedures and tools activities;***
- ***Transfers of knowledge to participants such as the business system manager, the maintenance teams, and the support or safety managers;***
- ***As necessary, coordination with the supplier in order to install upgrades and perform troubleshooting activities***

Designation of the business system management group resources required to participate in the various control activities.

[Enter content here]

An example Support Plan Template is provided at the end of this template.

4. Communication Plan

4.1. Communication Plan

Expected results, components to be installed, sequence of activities, and initiatives to be carried out within the framework of the communication aspect of the proposed releases.

Specification of resources required to distribute the release information.

[Enter content here]

4.2. Communication Plan Scope

Details pertaining to the context and the project phase for which the plan is produced.

Description of the changes that the communication plan supports.

Determination of the client groups that are affected by the release and that have release information requirements.

Determination of the information requirements of each of the client groups affected by the release, taking into account its features and its qualifications, the impacts of the change on these factors, its role and the complexity of its interactions with the system's unit tasks.

Specification of the timing of the information dissemination activities required for a smooth introduction of the change in the organization.

Determination of the information sessions required.

Depending on the size of the change project, details regarding the eventual integration of the communication in a larger scale plan.

[Enter content here]

4.3. Communication Content

Themes covered by the communications.

Specific messages for each client group.

Details on the preferred times to convey messages, the target dates, frequency, and duration of messages.

Sources of information to be used by the change agents: deliverables, reports, and documents. If necessary, mention any limitations on the use of a source document, such as its status (e.g. revised, approved).

[Enter content here]

4.4. Communication Methods and Tools

Description of the transmission and distribution mechanisms to be used or promoted through the presentations, information meetings, reusable or specific publications, couriers, internet or intranet sites, etc.

Definition of the media, as well as the presentation standards, templates, and logos to be used for the different media.

Definition of the conditions for access to the communication material by the change agents and, if applicable, by the final addressees.

Description of the applicable control and approval processes within the framework of the communication plan.

Statement of the constraints and standards to be met in terms of:

- ***availability of the appropriate space and material at the various sites;***
- ***travel, accommodation, and meal budget;***
- ***allocation of expenses.***

[Enter content here]

4.5. Communication Schedule

Presentation of the schedule of communication activities and initiatives through one or more charts (Gantt or other type) listing:

- ***the logical sequencing of the communication activities and initiatives;***
- ***the duration of these activities and the dates when they will take place;***
- ***the participant groups concerned (client groups and change agents);***
- ***the pivotal dates marking, in particular, synchronization with other plans such as the site preparation and installation plan, the training plan, or the test plans.***

[Enter content here]

5. Test Plan

5.1. Test Plan

Testing is accomplished at regular intervals in the development cycle. Some of the testing phases that may apply are unit, system, integration, regression, and user acceptance testing:

- ***Unit testing – tests the smallest pieces of the deployment;***
- ***System testing – tests multiple units to make sure they function properly as a system;***
- ***Integration testing – tests the system to make sure it functions properly in the environment;***
- ***Regression testing – re-running test plans because a change that was implemented could have impact in other areas;***
- ***User Acceptance Testing (UAT) – normally an end-to-end test completed by the customer.***

[Enter content here]

5.2. Scope of Test Plan

Details pertaining to the testing.

Description of the changes that the test plan supports.

Determination of the appropriate parties to conduct the testing.

Determination of the detailed testing steps to be completed.

Specification of the timing of the testing activities required.

[Enter content here]

5.3. Tracking of Testing

Appropriate bug tracking should be developed to ensure test failures are tracked, corrected, and retested.

An example Test Plan is provided at the end of this template.

An example Test Case Log is provided at the end of this template.

An example Traceability Matrix is provided at the end of this template.

[Enter content here]

6. Training Plan

6.1. Training Plan

Expected results, components to be installed, sequence of activities and initiatives to be carried out within the framework of the training aspect of the concerned change.

Definition of the controls used to verify that the plan is being followed. Specification of the resources required for imparting the training concerning the release.

[Enter content here]

6.2. Scope of Training Plan

Details pertaining to the context and the project phase for which the plan is produced.

Description of the changes that the training plan supports.

Determination of the client groups that are affected by the release and that have general or specific training requirements concerning the use, operation, support, or maintenance of the release.

Determination of the training requirements of each of the client groups affected by the release, based on its features and qualifications, the impacts of the change on these factors, its role, and the complexity of its interactions with the system's unit tasks.

Specification of the timing of the training activities required for a smooth introduction of the change in the organization.

Determination and definition of the necessary learning events.

Depending on the size of the change project, details on the eventual integration of the training in a larger scale plan.

[Enter content here]

6.3. Training Program Description

For each learning event, description of the learning objectives in terms of content, theme, and type of knowledge to be acquired.

For each learning event, description of the learning objectives in terms of the desired level to be acquired on a scale of competence.

Description of the proposed training program with regard to the target client groups.

Statement of the duration allotted to the various programs.

Description of the content, themes, and types of knowledge dispensed through the various learning events.

Definition of the prerequisites that the participants must meet before beginning a learning event or program.

[Enter content here]

6.4. Training Schedule

Presentation of the schedule of learning events through one or more charts (Gantt or other type) listing:

- ***The logical sequencing of the learning events;***
- ***The duration and dates of these activities;***

- ***The participant groups concerned (client groups and trainers);***
- ***The pivotal dates marking, in particular, synchronization with other plans such as the site preparation and installation plan, the communication plan, or the test plans.***

7. Finish / Closing Plan

7.1. Document the Release

It is important to capture as much data about the release as possible. Some of the critical documentation could be architecture, CMDB, security, versioning, issues, testing, and cost data.

[Enter content here]

7.2. Track and Resolve Issues

A key piece of a successful release is to clean up bugs or other issues that result from the release. Use as issue log to track and report on issue resolution after the release.

- ***An example Issue Log is provided at the end of this template.***

[Enter content here]

7.3. Close

Document lessons learned. The lessons learned session does not have to wait to the end of the release. If a release is phased, you will want to conduct a lessons learned at the completion of each phase in hopes to improve the next release phase. The lessons learned document should be completed and posted where others can benefit from it.

[Enter content here]

8. Representative Release Implementation Schedule

Group	Contents							
	Release Name/ID	Original Date	Expected Date	Actual Date	Defects	Changes	Type	Status

9. Representative Risk Log

Risk Log

Impact / Probability Legend	
	High
	Medium
	Low

Risk I.D. #	Description of Risk	Impact	Probability	Date	Identified by	Mitigation
	(sample)					
	(sample)					

10. Representative Test Plan

Test Plan

1. Introduction

Description of this Document
Related Documents
Schedule and Milestones

2. Resource Requirements

Hardware
Software

- Test Tools

Staffing

- Responsibilities
- Training

3. Features To Be Tested / Test Approach

New Features Testing
Regression Testing

4. Features Not To Be Tested

5. Test Deliverables

6. Dependencies/Risks

7. Entrance/Exit Criteria

11. Representative Test Case

<Project Name> Test Cases

Test Case Name	Test Case	Expected Results	Actual Results	Tester/Date	Tester Comments	Pass / Fail	Developer Recode Comments	Retest Comments

12. Representative Traceability Matrix

Requirements Testing Matrix								
ID #	**Requirement Description**	**Test Scenario ID#**	**Test Scenario - How this requirement will be evaluated**	**Tester Name(s)**	**Requirement Performance (Pass/Fail)**	**Test Outcome Description**	**Bug/Defect Status**	**Bug Resolution**
1		T1						
2		T2						
3		T3						
4		T4						

13. Representative Support Plan Template

Support Plan Template

Project Name:

Department:

Focus Area:

Prepared By

Document Owner(s)	Project/Organization Role

Project Closure Report Version Control

Version	Date	Author	Change Description

Note For standard sections of the Support Plan template that have been excluded from the present document, the section headings have been moved to the Support Plan Sections Omitted list at the end.

TABLE OF CONTENTS

1 SUPPORT PLAN PURPOSE 18
2 SUPPORT PLAN DETERMINATION/CERTIFICATION....19
3 SUPPORT PLANNING DEFINITION 20
3.1 Define Support Approach....20
3.2 Roles and Responsibilities....20
3.3 Define Support Profile....21
3.4 Define Helpstar Support Information....22
3.5 Define Non-labor Resources 23
3.6 Define Support Assumptions....23
3.7 Define Support Risks and Mitigations 23
3.8 Define Support Agreements/Service Level Agreements....23
4 TOTAL COST OF OWNERSHIP 24
5 SYSTEM CAPACITY REQUIREMENTS 25
6 Systems Support Plan APPROVALS....25
7 APPENDICES....26
7.1 Operational Readiness Checklist....26
7.2 Support Plan Sections Omitted....27

1. SUPPORT PLAN PURPOSE

Support Plan Purpose
[**Replace this text with a support planning purpose statement for your project-specific needs, or use the following sample. ETS standards should be reviewed to determine appropriate support activities to ensure standards are met.**] The Support Plan provides a record of all support planning for project follow-on support including the planned support approach, the identification of a team of workers that possess the appropriate skill set (for internally supported systems), and a record of the non-labor resources (tools, equipment, process, training, and so forth) necessary for post project support.

2. SUPPORT PLAN DETERMINATION/CERTIFICATION

Answer the following questions to determine if a system support plan is required. Any yes answer to the questions will require completion of the appropriate sections of the support plan. If all questions are answered no then a plan is not required and just the certification statement must be signed and this document becomes a part of the official project documentation.

Question	Yes	No
Does this system require additional support staff?		
Does this system generate additional funding requirements to support?		
Does this system require additional training to support?		
Does this project materially affect any current support approach for this system?		

I certify that this project will not materially change the current support provided this existing system.

_____

Project Manager

3. SUPPORT PLANNING DEFINITION

3.1. Define Support Approach

Define Support Approach
[**Replace this text with a high-level approach to providing follow-on support following system deployment.** • **[Consider whether support can be provided by outside agencies.]** • **[Consider whether the system can be hosted by the vendor.]** • **[Consider if current staff has the required skills and if staffing levels are adequate to support system.]** • **[Consider the type of tasks to be performed, and the total effort required to perform them.]**

3.2. Roles and Responsibilities

Roles and Responsibilities
[**Replace this text with a description of the various roles required to support the system and the function area responsible for providing the support.**]

Role	Responsible Support Group
Application Development	
Server maintenance	
Application of Business rules	

3.3. Define Support Profile

Define Required Skill Sets

[**Replace this text with a required-skill list, arranged by function, in order to identify the types of resources required, skill sets, source and estimated monthly workload or modify the following sample table.**]

Function	Resource Type	Skill Set	Source	Estimated Cost	FTE	Monthly Workload (Hrs)
Problem analysis and software modifications	Developer	Visual Basic	Consultant	TBD		
Database maintenance and modifications	DBA	SQL	Internal Staff	Internal		
Business rules changes	Systems Analyst	Application Training	Business Unit	Internal		

3.4. Define Helpstar Support Information

Define Helpstar Support Information

[**Replace this text with supported functions, in order to identify the functional areas supporting the system components, support queues incident reports are assigned to, application names, support contact information if not maintained by ETS and the business individual responsible for the data in the database, if applicable or modify the following sample table. The information is required to initially identify system support responsibilities in the Helpstar system.**]

Support Function	Functional Area	Support Queue	Application Name (If applicable)	Application Support Contact	Database Owner
Software Problem analysis and modifications					
Database maintenance and modifications					
(If Vendor Supported) Software Problem analysis and modifications					

3.5. Define Non-labor Resources

Define Non-labor Resources
[Replace this text with a list of non-labor resources required for on-going support—for example, licensing, hardware replacement, software and hardware maintenance. Additionally, system documentation to include technical and user manuals, system diagrams, source code, and hardware/software configuration settings.]

3.6. Define Support Assumptions

Define Support Assumptions
[Replace this text with a definition of the support needs assumptions identified during support approach decision.]

3.7. Define Support Risks and Mitigations

Define Support Risks and Mitigations
[Replace this text with a list of support risks and mitigations. Mitigations may include:] • [**Selection of vendor support, along with financial requirements.**] • [**Add additional time for knowledge transfer for which assigned resources have known skill deficiencies.**] • [**Add time for negotiating support agreement before project completion.]** • [**Add time and resources for training when no appropriately skilled resource is available.**]

3.8. Define Support Agreements/Service Level Agreements

Define Support Agreements/Service Level Agreements
[Replace this text with reference to any required maintenance agreements, service contracts or service level agreements (SLA) with vendors required for support. If a Service Level Agreement doesn't exist with the Application owner, a SLA should be established. Included should be contact information and procedures required to engage support. Additionally, the notification process, approval authority for downtime requests, and the scheduled maintenance windows should be established.]

4. TOTAL COST OF OWNERSHIP

Define 5 Year Total Cost of Ownership

[**Replace this text with the cost of Hardware replacement, Software licensing, Maintenance support for Hardware and Software, any contracted support by year, back-up system tape requirements, etc., up to five years, and the cost center responsible for budgeting the costs or modify the following sample table.**]

Requirement	Year 1	Year 2	Year 3	Year 4	Year 5	Total	Cost Center
Server Replacement							
Software Maintenance SQL Server Enterprise							
Application Support							

5. SYSTEM CAPACITY REQUIREMENTS

System Capacity Requirements

[**Replace this text with a description of the projected capacity needs over the next five years or modify the following table.**]

Requirement	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Production Disk Space						
Back-up storage requirements						

6. Systems Support Plan APPROVALS

Prepared By _____

([**Job Title**])

Approved By _____

([**Job Title**])

_____

([**Job Title**])

_____

([**Job Title**])

Approval Date _____

7. APPENDICES

7.1. Operational Readiness Checklist

Operational Readiness Checklist	Status
I. Security	
1. Was initial Security Assessment completed and issues remediated?	
2. Has the level of event detection/monitoring and response level been identified according to the system/application classification?	
3. Have security roles, permissions and authorizations been assigned to provide adequate logical access control?	
4. Have physical access controls been put into place, as required?	
5. Have required access control documents been approved and on file for vendor required access?	
6. Have patch management requirements been identified and responsible support groups notified?	
II. Process	
1. Have key stakeholders been identified for notification of system outages?	
2. Have relevant support information been put into the Helpstar Knowledge Base?	
3. Are any needed categories been added to Helpstar as appropriate?	
III. Sustainability	
1. Have appropriate asset information been entered into the asset database?	

2. Have the appropriate servers/databases been included in the back-up schedule?

3. Has new system/application been added to the DR plan?

4. Has the required support costs been added to the appropriate budgets?

5. Have required system support documentation been delivered and made available to appropriate support teams?

6. Have support personnel had all appropriate technical training?

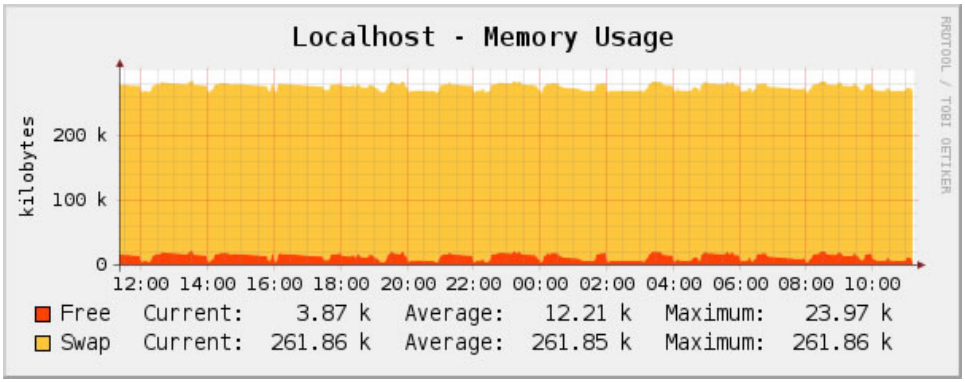
7.2. Support Plan Sections Omitted

- [**Omitted section**]
- [**Omitted section**]

Appendix E: Capacity Management Data Gathering Graphical Samples

Graphical models for this data may come from a variety of sources including system software, such as Windows Task Manager, or others such as Cacti, Ciscoworks, and Sysinternals.

Sample Graphs:



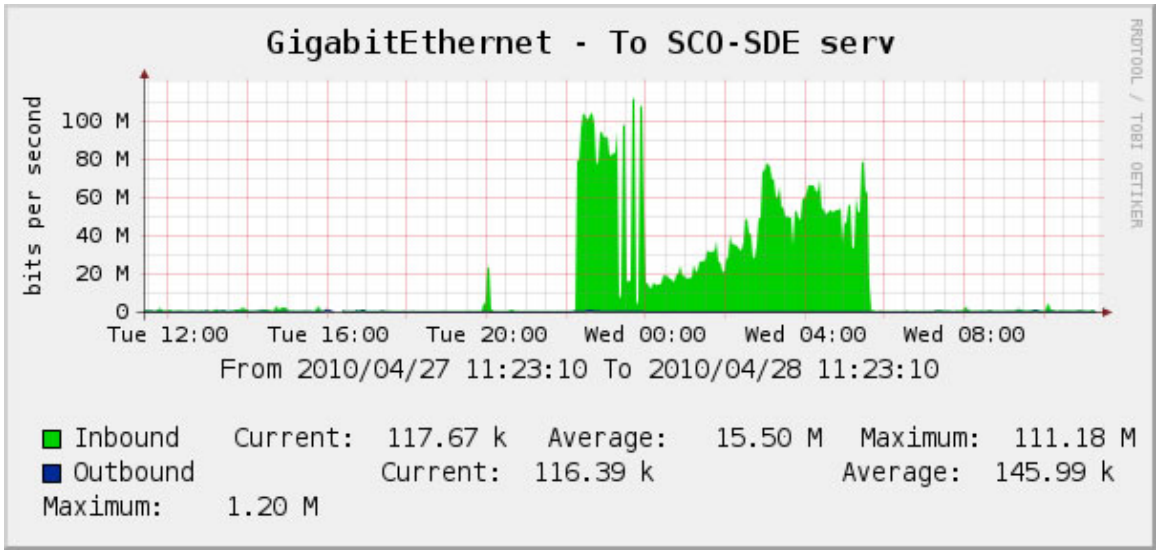
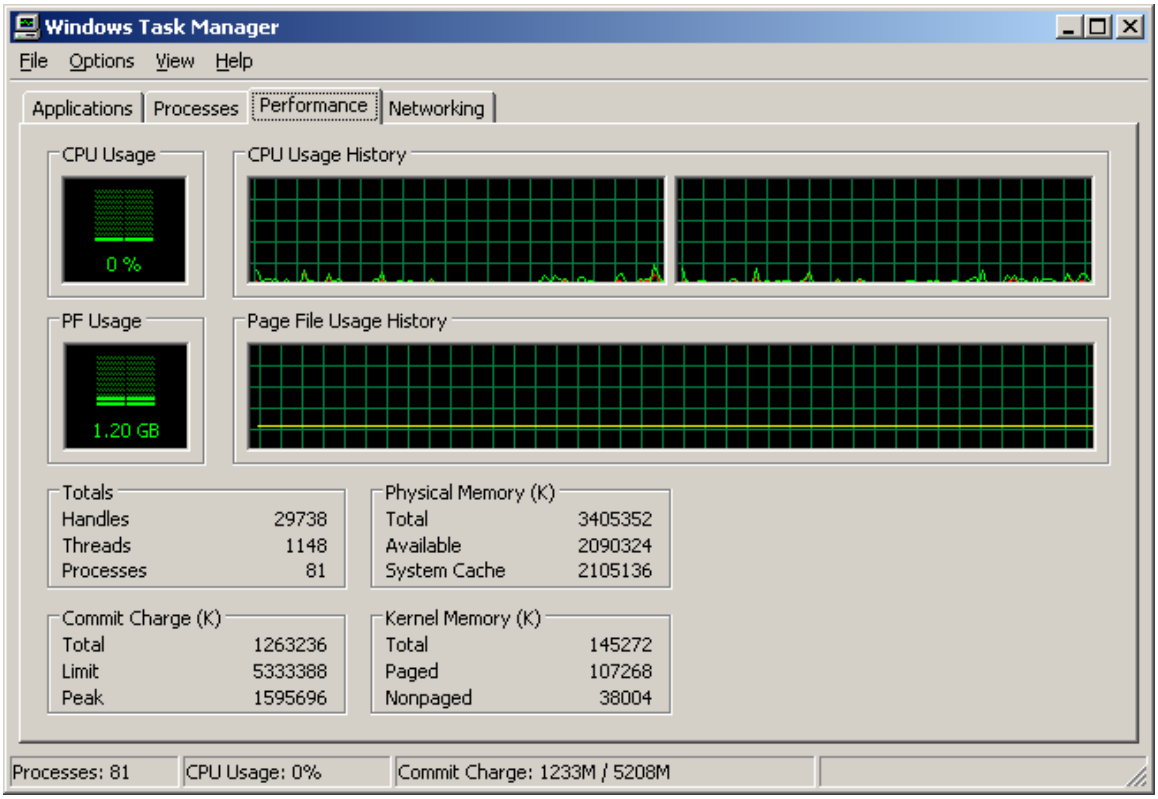
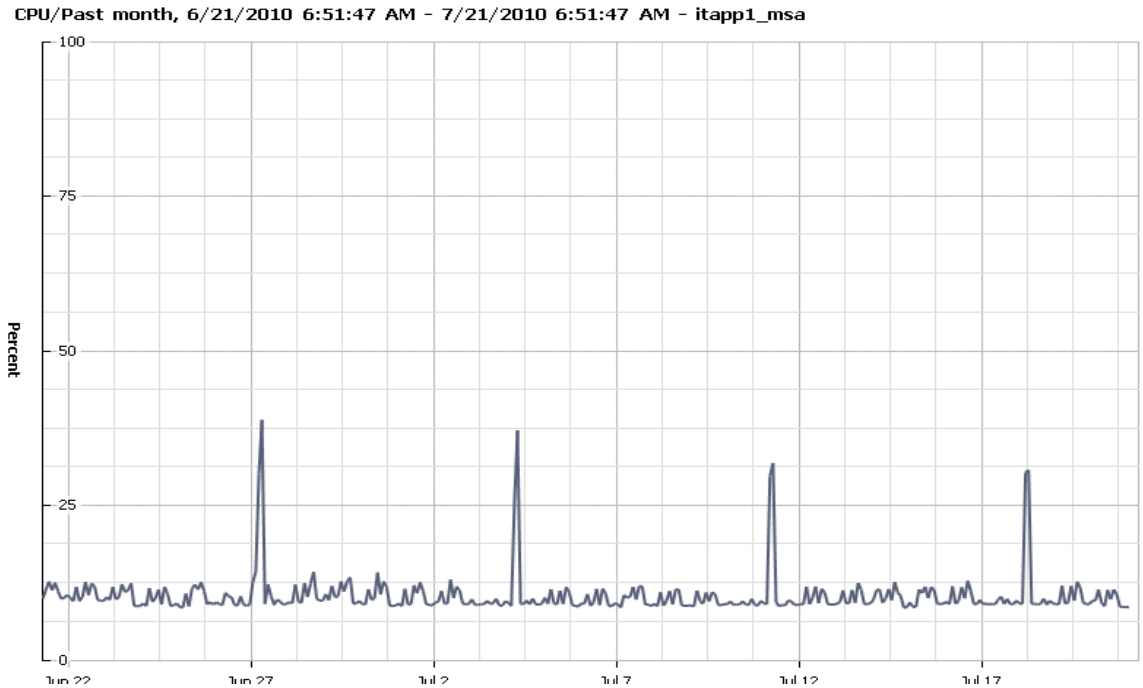


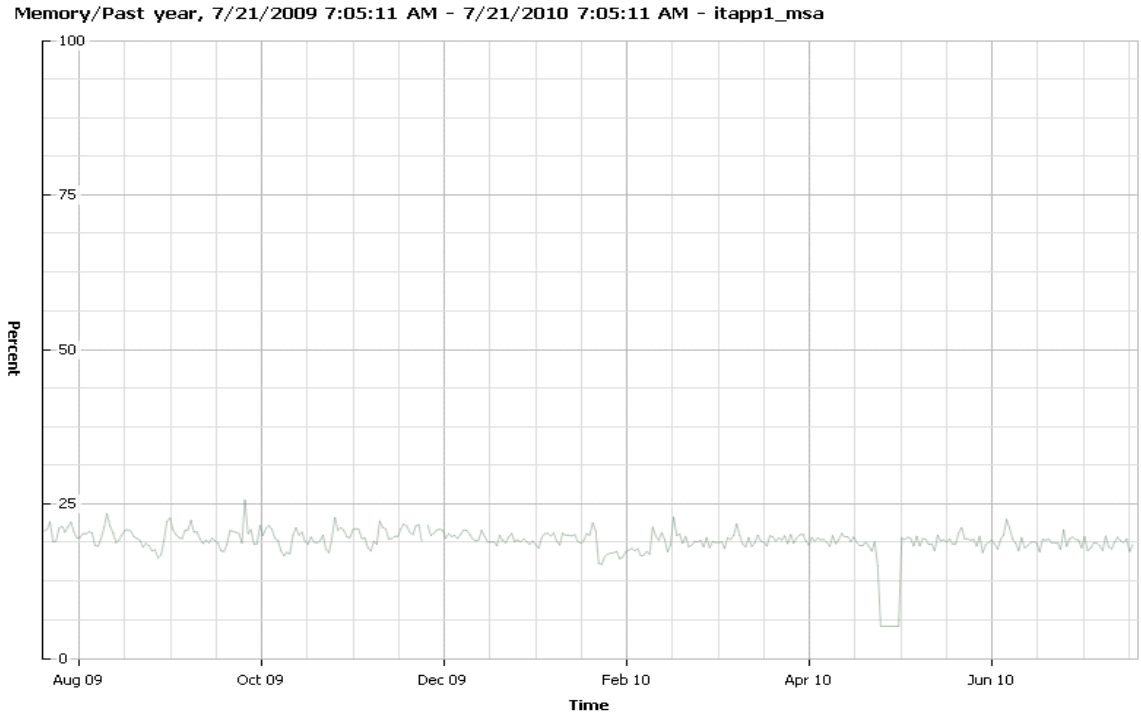
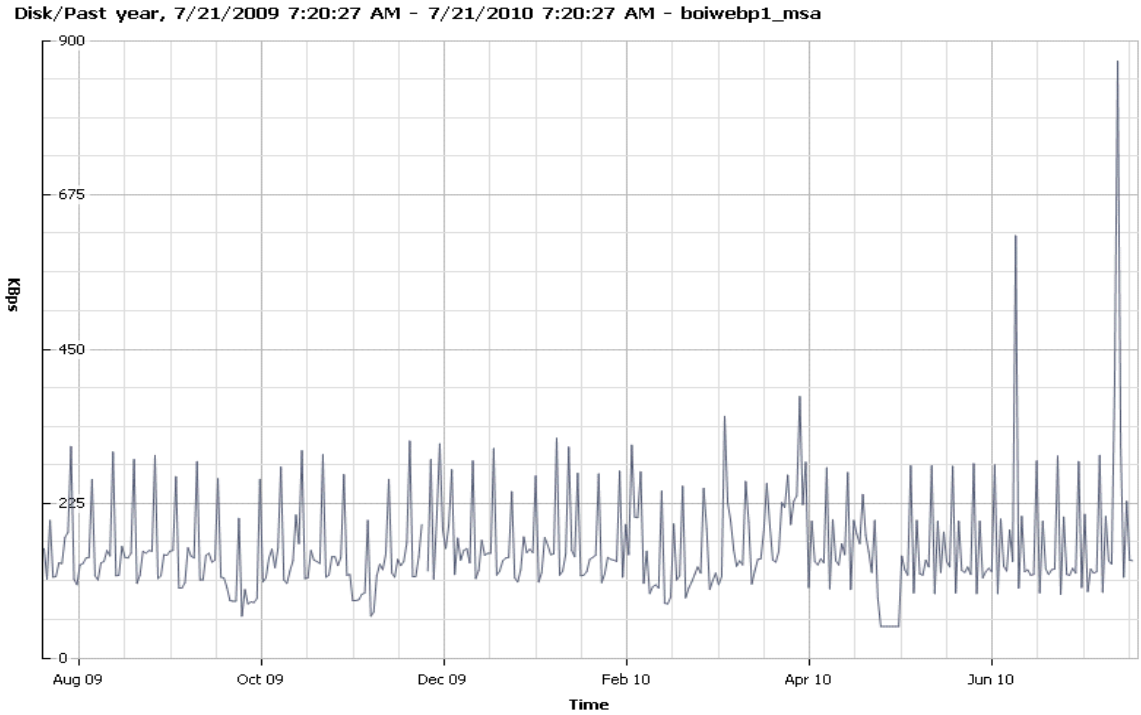
Figure 1 & 2 (above). From Cacti



Graphs showing CPU% usage over last year.



Graph showing memory % usage over last year.



Graph showing Disk space usage over last year.