
Facilities Management Policy and Procedures

Initial Draft

This document contains trade secrets and proprietary information belonging to <company name> International. No use or disclosure of the information contained herein is permitted without the prior written consent of <company name> International.

<company name>
All rights reserved

All trade names, trademarks, or registered trademarks are trade names, trademarks, or registered trademarks of their respective companies.

The computer file for this document is *FacilitiesManagementPolicyDraft12.doc*

The owner of this document is .

Document Review

Review Milestone	Date	Comments
Peer		
Preliminary Design Review (PDR)		
Critical Design Review		
Acceptance Review		
Release		

Document Revisions

Version	Date	Revisions
Initial Draft	5/26/00	Initial Draft

<company name>

Table of Contents

1 INTRODUCTION.....	1
1.1 FACILITIES MANAGEMENT OVERVIEW.....	1
1.2 AUDIENCE.....	2
2 POLICY.....	3
2.1 ROLES AND RESPONSIBILITIES.....	3
3 PROCESS.....	6
3.1 DEVELOPING BASELINE REQUIREMENTS.....	6
3.2 MANAGING RESOURCES.....	7
3.3 COMPLIANCE AND AUDITING.....	7
3.4 CORRECTIVE MEASURES.....	8
4 PROCEDURES.....	9
4.1 DEVELOPING BASELINE REQUIREMENTS.....	9
4.2 MANAGING RESOURCES.....	9
4.3 COMPLIANCE AND AUDITING.....	10
4.4 CORRECTIVE MEASURES.....	10
4.4.1 Risk and Impact Analysis.....	11
APPENDICES.....	12
RELIABILITY, COST AND SERVICE FACTORS.....	12
MEAN-TIME-BETWEEN FAILURE METRICS.....	12
MEAN-TIME-TO-REPAIR METRICS.....	12
SERVICE LEVEL AGREEMENT REQUIREMENTS.....	13
WARRANTY ISSUES.....	15
SERVICE LEVEL OBJECTIVES.....	15
EXPECTED SAVINGS AND COST/BENEFIT.....	19
5. AUDITING CHECKLISTS.....	20
PHYSICAL FACILITIES CHECKLIST.....	21
FIRE DAMAGE.....	22
AIR CONDITIONING.....	24
ACCESS CONTROL.....	25

1 Introduction

Facilities management addresses the maintenance and upkeep of physical facilities. This policy and procedures manual is focused on data center and equipment facilities.

1.1 Facilities Management Overview

Effective facilities management is the foundation of meeting service level objectives for operational support systems (OSS), telecommunications switching equipment and network infrastructure. These systems are the cornerstone of services offered to <company name> customers and must be housed in facilities that safeguard their security and integrity.

The following are critical success factors for facilities management:

Table 1 - Facilities Management Critical Success Factors

Critical Success Factor	Consequence of Not Meeting the Critical Success Factor
Compliance with national, state and local building and fire codes	Facility is at risk of being shut down by local authorities, which will cause disruption of services until all non-compliance items and discrepancies can be rectified. This event has the potential to result in revenue loss or erosion of <company name>'s customer base.
Adherence to established standards for cabling, heating, ventilation and air conditioning (HVAC), electrical, and building characteristics (weight distribution, access, equipment placement, etc.)	Non-standard implementations or installations can result in diminished performance, safety hazards, fire hazards and risk to equipment due to insufficient resources with which to support the OSS, telecommunications switching equipment and network infrastructure. Additional risks include structural damage due to improper equipment weight distribution, overheating due to insufficient HVAC resources, and inability to access key systems, subsystems and components in an emergency.
Safety	Potential for risks with consequences ranging from equipment damage to injury or loss of human life. Safety is closely related to compliance with national, state and local building and fire code critical success factors.
Support for disaster recovery and business resumption planning, policy and procedures	If facilities management is not aligned with disaster recovery and business resumption planning there could be either duplication of effort between the functions supporting facilities management and disaster recovery/business resumption planning, or gaps in <company name>'s plans for both areas leaving exposures.
Physical security	There are a number of risks and exposures to <company name>'s facilities. Specifically, all facilities supporting OSS, telecommunications switching equipment and network infrastructure are potential targets for vandalism, theft and attacks motivated by political or special causes. Moreover, facilities have the potential to be targets for industrial espionage.

1.2 Audience

The intended audiences for facilities management processes include:

- Facilities manager
- Data center manager
- Network and infrastructure manager(s)
- Security manager
- Operations manager
- Disaster Recovery/Business Resumption Manager
- Internal auditors

Specific roles and responsibilities for the intended audience of this document is provided in Section 2.1, Roles and Responsibilities.

2 Policy

The following is <company name> Communications policy for facilities management:

1. Facilities housing data centers, switches, other operational support systems (OSS) or network infrastructure will:
 - Comply with national, state and local building and fire codes.
 - Comply with Americans with Disability Act (ADA) public law with respect to facilities.
 - Adhere to established standards for cabling, heating, ventilation and air conditioning (HVAC), electrical, and building characteristics (weight distribution, access, equipment placement, etc.).
 - Be operated and maintained in accordance with best practices for safety.
 - Provide support for disaster recovery and business resumption planning, policy and procedures.
 - Have in place access controls, inspections and audits that are in keeping with best practices for physical security.
 - Be routinely cleaned and maintained with respect to a clean, uncluttered and trash-free environment.
 - Be proactively managed using a planned maintenance program and effective control over HVAC and electrical resources.

2.1 Roles and Responsibilities

Table 2 - Facilities Management Roles and Responsibilities

Role	Responsibility
<p style="text-align: center;">Facilities manager</p>	<ol style="list-style-type: none"> 1. Overall maintenance of all physical facilities 2. Managing planned maintenance for all physical facilities 3. Maintaining a resource budget for all environmental controls and electrical systems (i.e., total available power and environmental resources minus equipment using these resources will provide a budget of available resources. For example, if a facility has the capability of handling 100,000 BTUs of heat dissipation to keep the facilities at a constant 70°F and existing equipment puts out 70,000 BTUs, then the resource budget is 30,000 BTUs 4. Ensuring that all facilities comply with all applicable codes and laws (i.e., building and fire codes, ADA, etc.) 5. Forecasting additional resource requirements based on inputs from the data center manager, Switch Engineering, Operations Manager and other sources of information available from business units

Continued on next page

Table 2 - Facilities Management Roles and Responsibilities (continued)

Role	Responsibility
Data center manager	<ol style="list-style-type: none"> 1. Manages key access entry into the facilities, including ensuring that all visitors are escorted and sign a visitor log. In the case of visitors who have been authorized to access the facilities unescorted (third-party vendors on access lists, field engineers, etc.) that there is a record of their visit. 2. Responsible for enforcing security policies and procedures, and assisting the <company name> Security Manager in identifying exposures and risks with respect to data center operations,. For example, challenging unauthorized personnel who enter the operational premises in violation of security policy. 3. Develop, implement and manage an asset control process that provides for the identification and tracking of all physical assets under their area of cognizance. This includes serial numbers, configuration baselines, asset identification, and physical operating characteristics. Physical operating characteristics include power requirements (including stand-by power sources), BTU requirements, weight and load distribution requirements, physical interfaces (network infrastructure). 4. Providing the facilities manager with physical operating characteristics for planned hardware platforms (weight, power, HVAC and special installation requirements). 5. Assisting the Disaster Recovery/Business Resumption Manager with planning and systems tests and evaluation in support of disaster recovery and/or business resumption planning. 6. Providing the network and infrastructure managers with list of required physical and logical interfaces (including protocols, TCP/IP port numbers, etc) for connecting data center assets to the <company name> intranet, the Internet or other systems to which data center equipment needs to be interfaced (i.e., provisioning systems to switches, etc.).
Network and infrastructure manager(s)	<ol style="list-style-type: none"> 1. Providing the facilities manager with physical operating characteristics for planned communications hardware (weight, power, HVAC and special installation requirements) and cabling requirements. 2. Ensuring that planned demarcations between <company name> networking and communications infrastructure and third part service providers comply with service provider interface specifications and that the interface specifications are consistent with technical standards and [any] applicable fire, safety and building codes.
Security manager	<ol style="list-style-type: none"> 1. Establishing policies and procedures for physical security. 2. Providing the facilities manager with a list of physical security devices that need to be installed and implemented. 3. Providing the data center manager with requirements and procedures for maintaining physical security for the data center. 4. Coordinating security inspections and audits with the operations manager.
Operations manager	<ol style="list-style-type: none"> 1. Ensuring that physical operating characteristics are provided to the facilities manager in accordance with mutually agreed upon lead times. 2. Enforcing compliance with physical security policies and procedures that are established by the security manager. 3. Ensuring that disaster recovery/business resumption requirements are communicated to data center, network and infrastructure, and facilities managers. 4. Assisting the disaster recovery/business resumption manager with coordinating system tests and evaluations that involve facilities and infrastructure. 5. Assisting internal auditors by making facilities and personnel available for audits with respect to facilities.

Continued on next page

Table 2 - Facilities Management Roles and Responsibilities (continued)

<p>Disaster Recovery/Business Resumption Manager</p>	<ol style="list-style-type: none"> 1. Developing physical facility requirements that support disaster recovery/business resumption objectives (i.e., specifying requirements for redundant or secondary power sources, facilities emergency access, etc.). 2. Providing requirements to (1) operations manager and (2) facilities manager.
<p>Internal Auditors</p>	<ol style="list-style-type: none"> 1. Scheduling any internal audits of facilities and/or facilities security with the operations manager. 2. Conducting internal audits in accordance with <company name> corporate standards, methods and procedures for internal auditing of facilities and physical security.

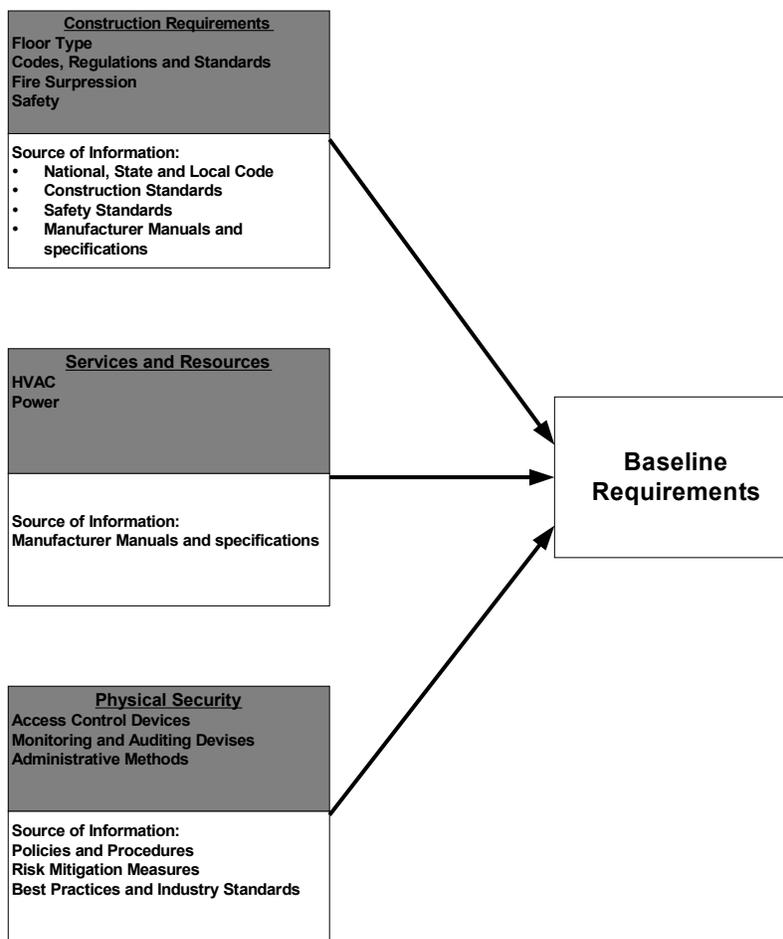
3 Process

Facilities management consists of the following processes:

1. Developing baseline requirements.
2. Managing resources.
3. Compliance and auditing.
4. Corrective Measures

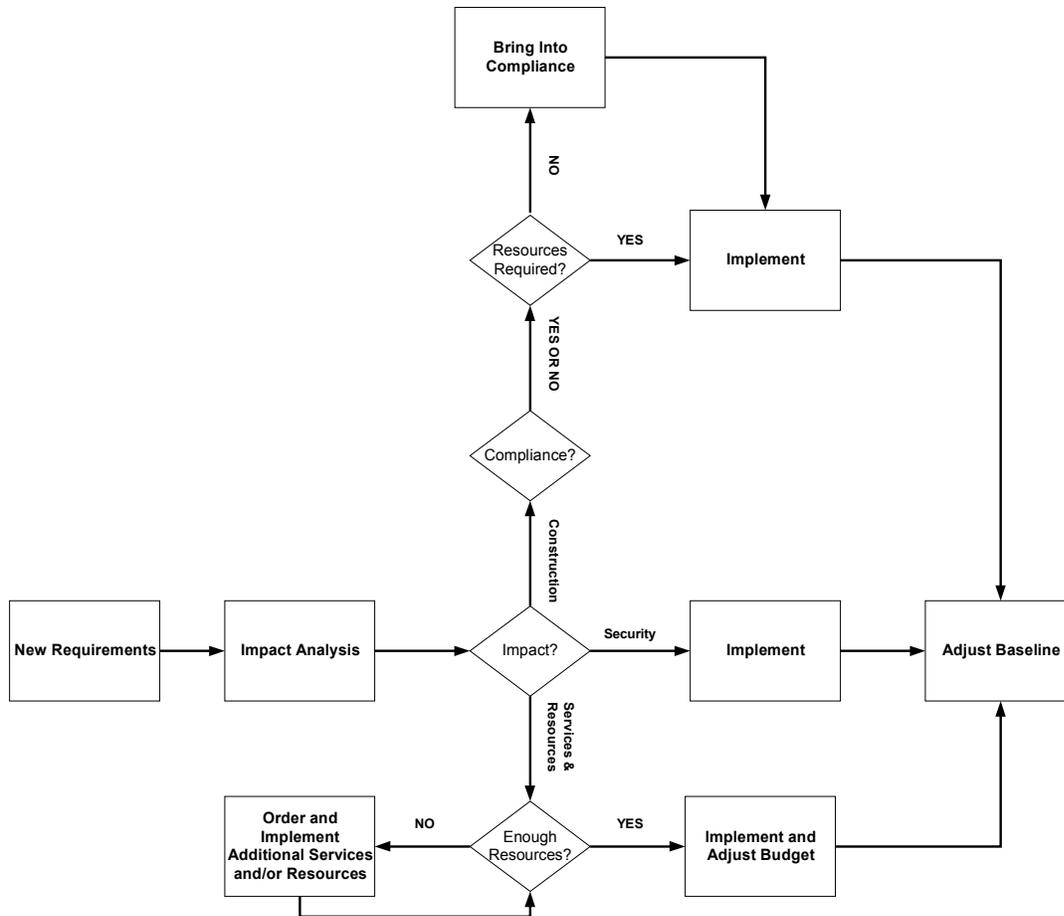
3.1 Developing Baseline Requirements

Baseline requirements encompass all requirements for services and resources (HVAC, power), construction requirements, physical security devices and methods, and compliance with codes, regulations and standards. This process is depicted in the following diagram:



3.2 Managing Resources

This sub process begins with the baseline, which should be designed to accommodate initial requirements for construction, services and resources, and physical security. As additional requirements emerge, such as adding services, network infrastructure, modified security standards, etc., an impact analysis is performed to determine if the baseline can support the new requirements. If not, additional resources are ordered and implemented to support additional requirements. This is depicted in the following diagram:



3.3 Compliance and Auditing

This sub process is ongoing and is performed at intervals to be determined by the following process owners:

1. Facilities Manager – audits for compliance with codes, regulations and standards and conducts safety inspections.
2. Security Manager – audits for compliance with security policies and procedures.

3. Disaster Recovery/Business Resumption Manager – audits for compliance with disaster recovery and business resumption plans.
4. Internal Auditor(s) – audits for compliance with <company name> internal controls.
5. Operations Manager – Audits data center manager operations, processes and procedures to ensure compliance with facilities management policy.

3.4 Corrective Measures

Identification of discrepancies and out of compliance facilities, processes or procedures will come from one of five sources:

1. Security Manager.
2. Disaster Recovery/Business Resumption Manager.
3. Internal Auditor(s).
4. Outside regulatory agencies (local building inspectors, fire safety inspectors, etc.).
5. Internal reports from employees.

Responsibilities for correcting discrepancies or facilities, processes or procedures that are out of compliance with any governing code, standard, regulation or policy are as follows:

1. Facilities Manager – corrects any discrepancy or compliance issue regarding physical facilities (includes construction, services and resources, and physical security devices).
2. Operations Manager – delegates responsibility for corrective action to data center manager within the scope of security and facilities, processes and procedures. The Operations Manager will retain accountability for ensuring that the corrective action has been accomplished.

4 Procedures

The following are general procedures to be used to manage the four facilities management processes that are presented in the preceding section.

4.1 Developing Baseline Requirements

When developing baseline requirements the process owners identified in Section 2.1 need to take the following factors into account:

1. Reliability – facilities supporting <company name>'s systems, OSS and network infrastructure need to be designed for maximum reliability because these systems are the foundation of the services that <company name> provides to customers. ^{Note 1}
2. Compliance with external standards, laws, regulations and codes (fire, safety, building, Americans with Disabilities Act (ADA) etc.).
3. Compliance with <company name> policies (security, internal controls, disaster recovery/business resumption plans, etc.).
4. Resources and services required to support existing and planned systems and equipment to be housed in the facilities (power, HVAC, fire suppression, etc.).
5. Construction requirements (load ratings for floors, space requirements, electrostatic suppression, etc.). Note: Construction requirements are closely related to compliance with external standards (list item 2 above) and resources and services (list item 4 above).
6. A life cycle approach should be taken to the development of the baseline. Factors should include reliability, costs, and service level management.

^{Note 1} See Appendices, 5 – *Reliability, Cost and Service Factors*.

4.2 Managing Resources

Resource Management procedures involves managing to budgets for power, HVAC and other resources that have been established in the initial baseline. The initial baseline will determine the amount of power and HVAC resources required. As new equipment is added resources will be consumed and the budget will decrease.

The facilities manager is responsible for employing the following procedures in support of managing resources:

1. Establishing the resource baseline.
2. Tracking resource consumption as new equipment is added.
3. Setting thresholds that will trigger ordering and implementing additional resources as new equipment is added.
4. Ensuring that thresholds leave a safety margin to accommodate emergent requirements that are dictated by business imperatives.

The data center and network and infrastructure managers are responsible for providing resource requirements to the facilities manager as soon as those requirements are known.

4.3 Compliance and Auditing

Roles and responsibilities for compliance and auditing have been identified in Section 3.3. Specific procedures for compliance and auditing will depend on the source of the audit. Government and regulatory agencies, such as building inspectors and fire/safety inspectors will conduct audits in accordance with checklists and criteria developed and defined by their parent agencies.

Internal audits will be performed in accordance with <company name> policies, methods and procedures for the type of audit being conducted. Refer to Appendices, *6- Auditing Checklists* for recommended internal auditing checkpoints.

4.4 Corrective Measures

The procedures for effecting corrective measures will be specific to the discrepancy or out of compliance condition that needs to be corrected. Factors include:

1. Priority – some discrepancies will be either minor in nature or not cost-effective to perform.
2. Time Requirements – typically, discrepancy and out of compliance conditions that violate laws and regulations will have a specific timeframe in which the discrepancy or condition must be corrected. Failure to meet these time requirements can result in fines or shutdown of facilities.
3. Risk and Impact – each major discrepancy needs to be evaluated based on its risk (probability of affecting <company name> business operations) and impact (the cost associated if the risk occurs). The risk and impact rating will determine the priority in which the discrepancy will be allocated resources and funds to correct. The next section provides more detail about risk and impact analysis.

4.4.1 Risk and Impact Analysis

:When evaluating the risk and impact of discrepancies and out of compliance conditions the following factors need to be examined:

1. Identification of risks associated with the discrepancy or condition.
2. Determination of probability and impact of risks (risk factor).
3. Plan to eliminate or mitigate the risks by correcting the discrepancy or condition.

A risk represents a condition that is subject to causing a failure or unexpected result. For example, if a critical piece of equipment server has a single power source, it is *exposed* to the possibility that if power fails business operations cease until power is restored. Preventing the risk associated with this particular exposure could be accomplished by using uninterruptable power supplies or an emergency generator.

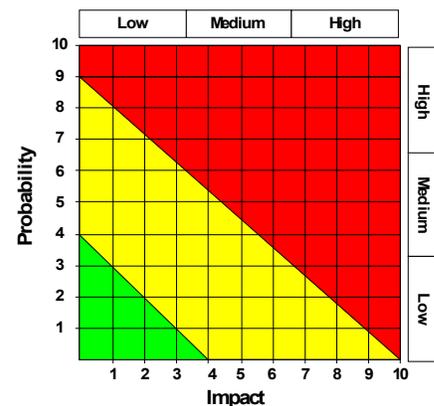
Other sources of risks include (but are not limited to):

1. Changes to building code.
2. Natural disaster.
3. New standards.

After risks have been identified, the next step is to determine both the probability of it occurring, and the impact it will have on the change implementation.

Determining probability need not be an exercise in mathematics - in many cases past experience will indicate whether the probability will be high, medium or low. In the matrix on the right, a low probability falls within the range of 0 to 30%; medium, 31-65%; and high, from 66-100% possibility of occurring.

A high probability of occurrence does not necessarily mean that the risk is significant. The true significance of a risk, called the *risk factor*, is derived by multiplying the probability by the impact of the risk on the project. For example, if the risk of losing power to a non-critical system every 6 years is 80% probable (high), but the impact is 2 (low), then the risk factor is 1.6 (the product of multiplying .8 by 2), which is also low. In this case the risk does not warrant much attention and would probably not rank high on a priority list. Conversely, if the same supported a mission-critical system and the impact was deemed to be 9 (high), then the risk factor will be a probability of .8 multiplied by 9, which equals 7.2 (high). This risk would need to be addressed immediately.



Appendices

Reliability, Cost and Service Factors

Mean-Time-Between Failure Metrics

MTBF is the *expected* elapsed time between failures, and is based on manufacturer data on failure rates. MTBF is computed as follows:

$$\text{MTBF} = \frac{\text{OPERATING HOURS}}{\text{FAILURES}}$$

This metric is an average, which means that variations in actual failure rates can occur in actual operation.

MTBF metrics are either provided in manufacturer or vendor specification sheets, or can be obtained from the vendor upon request. MTBF metrics need to be compared in the same manner as features and cost. However, because MTBF metrics are statistical there are misleading ways to present these metrics. The <company name> infrastructure is a collection of interrelated systems, subsystems and components; an MTBF metric for any one part of the infrastructure must be view within the context of how it affects the infrastructure as a whole. To illustrate how misleading it is to interpret an MTBF metric in isolation from the infrastructure itself, consider the following example.

Assume:

1. MTBF for a specific subsystem such a concentrator port at 500,000 hours (approximately 57 years)
2. 7x24 availability required (8,760 operating hours per year)
3. The population of ports as a subsystem of the same manufacturer/model concentrators is 1200, each with identical MTBF ratings

Computing the *system* MTBF requires multiplying 1200 (number of ports) x 8,750 operating hours to yield 10,512,000 cumulative operating hours. This number divided by the rated MTBF of 500,000 hours gives a failure rate of a little over 21 failures per year. This is vastly different from the perceived failure rate of once every 57 years.

Mean-Time-To-Repair Metrics

This is the average time to repair a system, subsystem or component. MTTR metrics that are provided by manufacturers and vendors are sometimes derived from data collected in a controlled environment. For example, an MTTR rating of 5 minutes

may be based on the actual time it takes a technician to perform the repair task in a test environment with all tools, spare parts and repair instructions pre-positioned.

In practice, an on-site technician responding to the same repair requirement would need to gather these materials, then go the equipment location to effect the repair make take much longer. For example, while the actual repair may still take 5 minutes, preparation and travel time may take an additional 30-90 minutes, depending on factors such as tool availability, parts provisioning and equipment location. These factors need to be taken into account when evaluating manufacturer and vendor specifications for MTTR.

A final note on MTTR importance: repair time will cost <company name> money in lost productivity (easy to measure) and lost opportunity (difficult to measure, but is a valid piece of the cost-of-downtime equation).

Service Level Agreement Requirements

Service level agreements (SLA) are guarantees that a certain level of service will be consistently maintained. SLAs are between manufacturer or vendors and customers, and between IT personnel managing the <company name> infrastructure and end users.

The basis for any infrastructure service level agreement is *availability*. The infrastructure should ideally be 100% available during normal hours of usage. However, because <company name> business objectives will require 7x24 availability achieving the ideal is not possible. There are two conditions that will govern availability:

1. Scheduled downtime for maintenance
2. Unplanned events (i.e., problems)

Scheduled downtime can be planned to occur when it will have the least impact on business operations and infrastructure availability. This period of unavailability can be negotiated between IT and the end user groups that will be affected by the temporary loss of service.

Unplanned events that deny service to end users is a breach of the SLA. Depending on the extend of service outage, an unplanned event can cost <company name> tens of thousands of dollars per hour. For example, if an outage on the <company name> backbone prevented 250 users¹ from doing their job, and the average fully loaded cost per user in salary was \$15.00, a problem that takes three hours to correct will cost <company name> \$11,250.00 in lost productivity. This does not take into account lost opportunities, overtime to make up necessary work, and the myriad of other factors that come into play when a necessary service becomes unavailable. Assuming 250 users @\$15.00/hour, each minute of downtime would cost <company name> \$62.50 in lost productivity.

¹*This example assumes that among the enterprise user population only 250 end users would depend on backbone availability at any given point in time. Actual usage patterns may vary.*

SLAs are also subject to negotiation between <company name> and vendors. For equipment that imposes a high cost of downtime to <company name> the negotiated SLAs should specify the maximum allowable time between the notification of a problem, and the time the vendor responds by commencing corrective action. Other SLA elements that need to be addressed are:

1. Responsibility for materials
2. Loaner equipment (especially when negotiating with vendors) in the event that repairs cannot be effected within a specified timeframe. For mission-critical equipment the recommended cut-off time is 4 hours
3. Penalty clauses to be invoked if the service level agreement is not fulfilled. Penalty clauses normally apply to vendors providing services; however, if <company name> develops charge-back policies in the future a penalty clause is also appropriate for internal service level agreements

In developing and negotiating service level agreements the primary consideration is cost. Parts provisioning, 7x24 support availability and minimum response times add to the cost of service. SLAs are one IT operations area where cost/benefit analysis can prove to be realistic because all factors are tangible.

A cost benefit analysis to determine the true value of a service level agreement will compare the cost of the service level objectives to the cost associated with service loss. The following simplistic formula summarizes SLA cost/benefit:

Cost of service loss x probability of occurrence > cost of SLA = value; conversely,
Cost of service loss x probability of occurrence < cost of SLA = negative value.

For example, if the cost of a three hour disruption of service is \$11,250.00, with a 10% probability of occurrence and the cost of the SLA is \$5,000.00 then the SLA has negative value because $\$11,250.00 \times .1 = \$1,125.00$. By paying \$5,000.00 for a service level agreement that protects against a three hour disruption in service the cost exceeds the potential loss by \$3,875.00.

The above example is provided to demonstrate a technique. It does not reflect the actual complexities in the cost/benefit analysis phase of developing and negotiating a service level agreement. Factors to be considered are:

1. Failure mode effects analysis (FMEA) of the infrastructure to determine failure points that will impact end users (both at the enterprise level and at the workgroup or subnetwork level)
2. Risk analysis of failure points, which will examine:
 - threat

- probability of occurrence
 - impact
3. Sensitivity to service loss from each threat by user population (i.e., backbone users tend to be a composite of numerous workgroups and labor categories; some workgroup fully loaded salary costs are higher than others--engineers vs. administrative personnel)
 4. Composite cost for loss of service for all failure points and probabilities

The above information will provide a true basis for determining the actual value of a service level agreement.

Warranty Issues

Equipment warranties should be carefully examined during the evaluation phase preceding acquisition, vendor selection or implementation of <company name> standards based on a particular manufacturer or vendor.

Key points to consider are:

1. Warranty term (three years should be the minimum acceptable period)
2. Remedies provided by the warranty (i.e., cross-shipped replacement, next day repair, parts and materials to rectify problem, etc.)
3. Exclusions, limitations and restrictions (i.e., if <company name> performs preventive maintenance and minor repairs will the warranty be voided? Are certain subsystems and components not covered by the warranty?)
4. Cost to extend and/or upgrade the warranty:
 - extensions increase the term of the warranty coverage
 - upgrades improve service level objectives
5. <company name> rights under the terms of the warranty (i.e., is the warranty enforceable?)
6. Does the warranty extend to software and firmware? (Most hardware depends to some extent on embedded firmware or externally loaded software; i.e., SNMP agents)

Service Level Objectives

Service level agreements are defined by service level objectives (SLOs). Important objectives that <company name> needs to consider include:

1. Hours of coverage, which are usually defined as either during the principal period of maintenance (PPM) or outside of the principal period of maintenance

2. Response to requests for service, measured in the elapsed time between when a call is placed and the time that the call is acknowledged
3. On-site response, which is the elapsed time between when a call is placed and the time that a support person arrives on site
4. Maximum time allowed to rectify problem; options include:
 - requirement that functionally equivalent loaner equipment be provided after a determined (or negotiated) period of systems unavailability
 - hot or cold standby equipment that can either be automatically switched into full operational service (or manually brought on-line)
 - acceptance of partial operational capabilities until full system availability is restored (i.e., interim use of 56K DDS on a DS1 backbone segment)

The most important issue when developing SLOs is to use system availability as the key performance indicator. System availability is a function of MTBF, operational time, total service time, and MTTR. The significance of MTBF, discussed in above, is readily seen in the following series of formulae for systems availability, measured in percent availability. Percent availability, expressed as A%, can be computed two different ways:

Method 1

$$A\% = \frac{\text{Operational Time}}{\text{Total Time}} \times 100$$

Applied to the infrastructure as a whole, assume that of the 8,760 hours of 7x24 operations per year, <company name> scheduled 16 hours of planned maintenance, and experienced no outages due to system problems. Using the above formula system availability would be:

Operational time: $8,760 - 16 = 8,744$

Total time: 8,760

$8,744/8,760 = 0.9981735159817$

$0.9981735159817 \times 100 = 99.81735159817$

or approximately 99.81% availability

Method 2

$$A\% = \frac{\text{Mean-Time-Between-Failures}}{\text{MTBF} + \text{MTTR}} \times 100$$

Assume:

1. True MTBF (cumulative effect as discussed above) rated at 3,000 hours using the MTBF formula:
2. 8,760 operating hours with 3 failures observed
3. MTTR of 60 minutes to correct each failure

$$\text{MTBF} = \frac{\text{Operating Hours}}{\text{Failures}}$$

Availability would be:

$$\text{MTBF} = 3,000 \text{ hours}$$

$$\text{MTTR} = 3 \text{ hours (60 minutes} \times 3 \text{ incidents)}$$

$$3,000 / 3003 = 0.999000999001$$

$$0.999000999001 \times 100 = 99.9000999001, \text{ or approximately } 99.9\% \text{ availability}$$

See table 1.2 for the relationship between percent availability and downtime per year (broken out in minutes, hours, days and weeks).

The following formulae will assist personnel responsible for facilities management in developing life cycle costs.

$$\text{FTE (maintenance)} = \text{CMM} + \text{PMM}$$

CMM is corrective maintenance manhours, and is computed as follows:

$$\text{CMM} = T \times 8760 \times \text{MTTR} \times A \times M$$

Where:

T = Total failure rate as number of failures per hour. This includes all failures.
(Equals 1 / Mean Time Between Failures)

8760 = Number of hours in a year

MTTR = Mean Time To Repair. The time in hours it takes to restore a subsystem or component to operating condition (MTTR can sometimes be found in maintenance documentation or specifications that accompany systems, subsystems or components; this rating may also be available from the manufacturer)

A = The number of personnel required to do the work.

M = The manhour rate (for <company name> personnel use the fully loaded rate; for third-party vendors use the hourly time and materials rate).

PMM is annual preventive maintenance manhours. This is based on all required and recommended preventive maintenance for a system, subsystem or component. The maintenance actions are normally listed in the maintenance manuals that

accompany the equipment. This information may also be available from the manufacturer. It is computed as follows:

$$\text{PMM} = \text{Number of times per year} \times \text{Manhours} \times M$$

Where:

Manhours = The number of manhours required to perform each preventive maintenance action.

M = The manhour rate (for <company name> personnel use the fully loaded rate; for third-party vendors use the hourly time and materials rate)

$$\text{FTE (operations)} = \text{Estimated number of FTEs required to operate system} \times 2088 \times M$$

Where:

FTE = The number of full time equivalents required to operate the system. Consideration the SLA that will be associated with the system, especially availability (i.e., is 7x24 manning required?). This number can be a fraction, such as .5 FTE.

2088 = Number of annual manhours per FTE.

M = The manhour rate (for <company name> personnel use the fully loaded rate; for third-party vendors use the hourly time and materials rate).

FTE (support) = Estimated number of FTEs required to provide tier 1 support. This cost should be provided by the <company name> help desk.

$$\text{Spare Parts Consumption} = \text{CMSP} + \text{PMSP}.$$

CMSP is Spare parts for corrective maintenance, and is computed as follows:

$$\text{CMSP} = T \times 8760 \times \text{Average corrective spares}$$

Where:

T = Total failure rate as number of failures per hour. This includes all failures. (Equals 1/Mean Time Between Failures)

8760 = Number of hours in a year

Average annual spares = Average spares needed for repair of the equipment - this information may be available from the manufacturer.

PMSP is Spare parts for preventive maintenance, and is computed as follows:

PMSP = Number of times per year x Average spare parts consumption per preventive maintenance action

Where:

Number of times per year is the frequency of each preventive maintenance action recommended or required by the manufacturer (this information is usually available in the maintenance manual that accompanies the equipment).

Average spare parts consumption per preventive maintenance action is the number of spare parts replaced (on average) or consumables used (on average) during each preventive maintenance action.

Expected Savings and Cost/Benefit

Expected savings is expressed as follows:

$$\text{Expected Savings} = (\text{CE} + \text{CA}) - ((\text{IC} + (\text{OC} \times \text{LC}))$$

Where:

CE is cost elimination over the life of the system - for example if the project results in a system designed to be in place for 5 years, and it eliminates cost items totaling \$1M/yr., then CE would be \$5,000,000.00. The period used in computing total CE is equal to the system's life cycle (see LC below)

CA is cost avoidance over the life of the system - an example of cost avoidance is a system with automatic features that replaces (or reduces) the number of operators; another example is a system with greatly reduced maintenance requirements, or a system that requires expensive proprietary parts being replaced with one that can be maintained and upgraded with commercial, off-the-shelf parts that are readily available on the open market (competition drives down prices, resulting in avoidance of premium prices)

IC is implementation costs, which is a one-time cost to implement the system (personnel and materials)

OC is operational and support costs per year - see Section 3.2.2.5.6.2 for a detailed description of typical operational and support cost line items

LC is the life cycle of the system - how long the system is expected to be in service (usually 3 to 5 years)

Cost/Benefit is the ratio of costs to expected savings and is expressed as follows:

$$\text{C/B} = ((\text{IC} + (\text{OC} \times \text{LC})) / (\text{CE} + \text{CA}))$$

See Expected Savings above for explanation of symbols.

5. Auditing Checklists

- a. Physical facilities
- b. Personnel with access
- c. Hardware
- d. Software
- e. Service personnel
- f. Files
- g. Internal audit controls
- h. Contingency plan(s)

PHYSICAL FACILITIES CHECKLIST

Water Damage Exposure

	YES	NO	N/A*
a. Have all overhead and underfloor steam or water pipes been eliminated (except for fire sprinklers or machine room requirements)?	_____	_____	_____
b. Are all electrical outlets under raised floor water tight?	_____	_____	_____
c. Are all exterior doors and windows waterproof?	_____	_____	_____
d. Do adjacent areas, restrooms, janitor room, etc. have adequate drainage to prevent overflow to computer room?	_____	_____	_____
e. Is paper stock stored in a water resistant area?	_____	_____	_____
f. If computer facilities are located below grade is a water detection system installed?	_____	_____	_____
g. Are large plastic sheets available to cover equipment for quick emergency water protection?	_____	_____	_____
h. Are openings sealed from upper floor or roof?	_____	_____	_____
i. Is computer located under rooftop cooling towers?	_____	_____	_____
j. Do you have drainage in computer room?	_____	_____	_____
k. Is there a flood control pump for below grade?	_____	_____	_____

Comments: _____

*Not Applicable

(Physical Facilities, contd.)

Fire Damage

	YES	NO	N/A*
a. Is the building housing the computer constructed of fire resistant and noncombustible material?	_____	_____	_____
b. Are combustible materials such as paper and other supplies stored outside of the computer area?	_____	_____	_____
c. Are tapes and disks stored outside of the computer area?	_____	_____	_____
d. Do you have a rated fireproof safe in the computer room for critical file storage?	_____	_____	_____
e. Are fire drills practiced periodically and individuals assigned responsibilities in case of fire?	_____	_____	_____
f. Are emergency phone numbers posted for fire, police, doctor(s), and hospital?	_____	_____	_____
g. Are computer and tape library protected from fire by use of overhead sprinklers, stand pipe hose, carbon dioxide, or halogenated agent?	_____	_____	_____
h. Are smoke detectors installed under the floor, in the ceiling and in the air ducts?	_____	_____	_____
i. Are smoke detectors serviced and tested on a scheduled basis?	_____	_____	_____
j. Do you have enunciator panels to assist in quickly locating fire or smoke in exposed areas?	_____	_____	_____

Comments: _____

*Not Applicable

(Physical Facilities, contd.)
 (Fire Damage, contd.)

	YES	NO	N/A*
k. Are floor tile removers readily available to expose fire or smoke under raised flooring?	_____	_____	_____
l. Are hand extinguishers strategically located around the area with location markers visible over high computer equipment?	_____	_____	_____
m. Have employees been instructed on how to use hand extinguishers?	_____	_____	_____
n. Are employees allowed to smoke in computer or tape library area?	_____	_____	_____
o. Do employees know the location of sprinkler shut-off valve?	_____	_____	_____
p. Are furniture and fixture of noncombustible material?	_____	_____	_____
q. Does emergency power-off also shut down the air conditioning or heating unit?	_____	_____	_____
r. Do you have emergency lighting in the computer environment?	_____	_____	_____
s. Does fire alarm sound locally, at the guard station, or police and fire department?	_____	_____	_____
t. Are watchmen schooled as to what to do about a fire during non-working hours?	_____	_____	_____
u. Would access to computer area, in case of fire, be restricted because of electrically controlled system?	_____	_____	_____
v. Do you have fire dampers in the ducts?	_____	_____	_____

Comments: _____

*Not Applicable

(Physical Facilities, contd)

Air conditioning

	YES	NO	N/A*
a. Is system dedicated to the computer area?	_____	_____	_____
b. Is remote air conditioning equipment secured?	_____	_____	_____
c. Are air intakes located above the street level or protected from air contamination?	_____	_____	_____
d. Is back-up air conditioning by use of a second compressor or chilled water available?	_____	_____	_____
e. Is the compressor and related air conditioning equipment serviced on a regular schedule?	_____	_____	_____
f. Is air conditioning complete with humidity control?	_____	_____	_____
g. Is air temperature and humidity recorded in computer operations?	_____	_____	_____
h. Are building engineers sensitive to the quick response required of computer operations?	_____	_____	_____
i. Is air conditioning alarmed in the event of failure?	_____	_____	_____

Comments: _____

*Not Applicable

(Physical Facilities, contd.)

Access Control

	YES	NO	N/A*
a. Is computer area visible from the street?	_____	_____	_____
b. If computer area is visible to the general public, are windows of non-breakable material?	_____	_____	_____
c. If the latter is so, is the fire department aware that windows are non-breakable in event of fire?	_____	_____	_____
d. Is the installation located in a high crime related area?	_____	_____	_____
e. Do site personnel consider the installation vulnerable to vandalism or a potential target because of the business conducted on the premises?	_____	_____	_____
f. Would site personnel evaluate the installation as high, medium, or a low risk center for attack?	_____	_____	_____
g. Does the site have 24 hour guard service?	_____	_____	_____
(1) For all entrances?	_____	_____	_____
(2) For the computer area only?	_____	_____	_____
h. Are TV cameras used in the computer area?	_____	_____	_____
i. Is the location of the computer services are displayed anywhere on the site, such as maps at entrance ways?	_____	_____	_____
j. Is a man trap for access used to get into the actual computer area?	_____	_____	_____
k. Are the number of doors leading into the computer area kept to a minimum?	_____	_____	_____
l. Who monitors the status of emergency exits?	_____	_____	_____

*Not Applicable

(Physical Facilities, contd.)

2. Access Control

	YES	NO	N/A*
a. Is computer area visible from the street?	_____	_____	_____
b. If computer area is visible to the general public, are windows of non-breakable material?	_____	_____	_____
c. If the latter is so, is the fire department aware that windows are non-breakable in event of fire?	_____	_____	_____
d. Is the installation located in a high crime related area?	_____	_____	_____
e. Do site personnel consider the installation vulnerable to vandalism or a potential target because of the business conducted on the premises?	_____	_____	_____
f. Would site personnel evaluate the installation as high, medium, or a low risk center for attack?	_____	_____	_____
g. Does the site have 24 hour guard service?	_____	_____	_____
(1) For all entrances?	_____	_____	_____
(2) For the computer area only?	_____	_____	_____
h. Are TV cameras used in the computer area?	_____	_____	_____
i. Is the location of the computer services are displayed anywhere on the site, such as maps at entrance ways?	_____	_____	_____
j. Is a man trap for access used to get into the actual computer area?	_____	_____	_____
k. Are the number of doors leading into the computer area kept to a minimum?	_____	_____	_____
l. Who monitors the status of emergency exits?	_____	_____	_____

*Not Applicable

(Physical Facilities, contd.)
 (Access Control, contd)

	YES	NO	N/A*
m. Are doors to computer area locked at all times?	_____	_____	_____
n. Is access to the computer area by use of key, magnetic card, or cipher lock controlled?	_____	_____	_____
o. Are access methods changed at regular intervals or after termination of an employee?	_____	_____	_____
p. Are dismissed employees of the computer environment removed immediately and guard personnel notified accordingly?	_____	_____	_____
q. Is the computer itself alarmed so as to notify guards of intrusion attempts?	_____	_____	_____
r. Is there stand-by power operated doors if normal power is off?	_____	_____	_____
s. Are security personnel notified of employees permitted access during non-working hours?	_____	_____	_____
t. Are records maintained of personnel who utilize the facility after normal working hours?	_____	_____	_____
u. Do site personnel "baby-sit" service personnel during non-working hours?	_____	_____	_____
v. Are all visiting personnel identified by badge when visiting the data processing area?	_____	_____	_____
w. Are operating personnel trained to challenge strangers without proper identification badges?	_____	_____	_____

Comments: _____

*Not Applicable

(Physical Facilities, contd.)

Electricity

	YES	NO	N/A*
a. Is uninterrupted power required at the site because of the nature of its activities?	_____	_____	_____
b. If the system requires motor generators, is there a back-up?	_____	_____	_____
c. How reliable is the local power supply; has reliability been checked?	_____	_____	_____
d. Have power sources been monitored with recorders to assure no electrical transients?	_____	_____	_____
e. In event of power failure, is there emergency lighting for removal of personnel?	_____	_____	_____
f. Are cipher doors and fire alarm systems backed up with battery in event of power failure?	_____	_____	_____
g. Is back-up power tested at regular intervals?	_____	_____	_____
h. Are lightning arrestors installed?	_____	_____	_____
i. Is there an emergency "power off" at all exits and within the computer center?	_____	_____	_____
j. Are emergency "power offs" protected against accidental activation?	_____	_____	_____

Comments: _____

*Not Applicable

(Physical Facilities, contd.)

Housekeeping

	YES	NO	N/A*
a. Is the underfloor kept clean of dust and dirt?	_____	_____	_____
b. Are wastebaskets of metal material with closing tops?	_____	_____	_____
c. Are wastebaskets dumped often enough to prevent overflow in the computer room?	_____	_____	_____
d. Is there a scheduled removal of empty paper boxes and waste paper?	_____	_____	_____
e. Are service personnel supervised at all times by a site representative?	_____	_____	_____
f. Is the computer room used to store stock or stationary?	_____	_____	_____
g. Is eating allowed in the computer room?	_____	_____	_____
h. Is smoking allowed in the computer room? If so, are ashtrays the type that extinguish cigarettes?	_____	_____	_____
i. Are employees held responsible for a clean working environment?	_____	_____	_____
j. Does management or supervision inspect areas for adherence to good housekeeping?	_____	_____	_____
k. Do site personnel themselves consider their computer area clean?	_____	_____	_____

Comments: _____

*Not Applicable

CHECKLIST FOR SERVICE PERSONNEL AND CONTRACTORS

	YES	NO	N/A*
a. Are custodial personnel controlled when servicing the secure area?	_____	_____	_____
b. Are unauthorized personnel required to wear identification to assure their entry has been approved?	_____	_____	_____
c. Are unauthorized personnel escorted when working in the secure area?	_____	_____	_____
d. Are secure area personnel instructed to challenge unidentified personnel in the secure area?	_____	_____	_____
e. Is a list of unauthorized personnel (exclusive of operations people on site) maintained?	_____	_____	_____
f. When the computer center is closed, do guards make key runs inside the center?	_____	_____	_____
g. Is there a rigid control center on keys to computer environment?	_____	_____	_____
h. Are computer room door locks changed from time to time to prevent normal custodial master keys from gaining entrance?	_____	_____	_____
i. Is there a log of unauthorized personnel who are admitted, with a notation as to reason for entry, time in, time out, and signature of person authorizing entry?	_____	_____	_____
j. Is identification with photo required of service personnel?	_____	_____	_____
k. Are vendor service personnel required to have background checks?	_____	_____	_____
l. Are custodial and maintenance personnel briefed on site security measures?	_____	_____	_____

Comments: _____

*Not Applicable

CONTINGENCY PLANNING CHECKLIST

	YES	NO	N/A*
a. Has top management, in conjunction with Data Processing management, set this contingency planning objectives?	_____	_____	_____
b. Does the contingency planning team consist of two or more permanent members such as:			
Computer Operations Staff	_____	_____	_____
Facilities Management	_____	_____	_____
Building Management	_____	_____	_____
c. Does the plan include participation on an "as required" basis from the following departments:			
Data processing operations	_____	_____	_____
Systems programming	_____	_____	_____
Applications programming	_____	_____	_____
Internal auditors	_____	_____	_____
Legal department	_____	_____	_____
Security/Fire/Safety staff	_____	_____	_____
Purchasing	_____	_____	_____
Insurance	_____	_____	_____
Real estate	_____	_____	_____
Communications	_____	_____	_____
Others (list in comments)	_____	_____	_____
d. Has the responsibility for each member of the contingency plan been defined?			
Primary action responsibility assigned?	_____	_____	_____
Coordination responsibility assigned?	_____	_____	_____

*Not Applicable

(Contingency Planning, contd)

	YES	NO	N/A*
e. Does the plan categorize disasters and provide specific plans for each level of potential disaster?			
Catastrophic	_____	_____	_____
Major	_____	_____	_____
Serious	_____	_____	_____
Limited	_____	_____	_____
f. Has an estimate of potential loss due to processing delay of critical reports been established in event of:			
Catastrophic disaster?	_____	_____	_____
Major disaster?	_____	_____	_____
Serious disaster?	_____	_____	_____
Limited disaster?	_____	_____	_____
g. Has a resource inventory been made to estimate the potential physical and/or process delay loss in each of the following areas:			
Equipment	_____	_____	_____
Data processing hardware	_____	_____	_____
Maintenance equipment	_____	_____	_____
Alternate site hardware	_____	_____	_____
Computer and components	_____	_____	_____
Terminal equipment	_____	_____	_____
Off-line equipment	_____	_____	_____
Furniture	_____	_____	_____
Office machines	_____	_____	_____
Preventative maintenance schedule	_____	_____	_____

*Not Applicable

(Contingency Planning, contd)

	YES	NO	N/A*
Alternate site software	_____	_____	_____
Maintained to meet site configuration modifications	_____	_____	_____
Reviewed and tested	_____	_____	_____
Stored in a secure environment	_____	_____	_____
Supplies			
Paper	_____	_____	_____
Forms	_____	_____	_____
Tape/Disks	_____	_____	_____
Cards	_____	_____	_____
Alternate site storage for:			
Tapes	_____	_____	_____
Disks	_____	_____	_____
Paper and forms	_____	_____	_____
Cards	_____	_____	_____
Emergency site(s) processing considerations at:			
Other owned/leased facilities under the installations control	_____	_____	_____
Other similar installations in the immediate area with whom contact could be authorized	_____	_____	_____
Computer manufacturer facilities	_____	_____	_____
Service bureaus in the immediate areas	_____	_____	_____

*Not Applicable