PSHS-MC

Information Systems Operations, Maintainance and Support

Roy Vincent L. Canseco © 2020 Manila

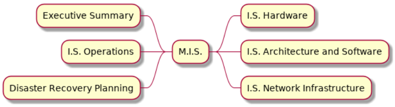
Revision 0.1
07.2020

Table of Contents

```
This is a draft verion.
```

1

Executive Summary


Executive Summary
I.S. Operations
Disaster Recovery Planning
M.I.S.
I.S. Hardware
I.S. Architecture and Software
I.S. Network Infrastructure

IT service management (ITSM) practices are important to provide assurance to users and to management that the **expected level of service** will be delivered. Service level expectations are ideally derived from the organization's business objectives and constraints. IT service delivery is a coordination of IS operations, IT services, and management of IS and the groups responsible for supporting them. IT services are built on service management frameworks (e.g. ITIL).

1.1. MIS Necessary Skills

In order to deliver and support IT services, a fair amount of skill in the following key areas should be present in the MIS Unit.

1. Management and Operations Skills
2. Software and Architecture Skills
3. Network Infrastructure Skills

    a. Wireless Technologies

    b. Secure Transmission

    c. Network Administration

    d. Internet Services

4. Hardware and Troubleshooting Skills

a. Server Setup

b. Workstation Maintenance

It is important to have a clear and agreed-upon measure of performance for these areas. This is where Service Level Agreements (SLA’s) are used.

1.2. Managerial Tasks

The manager of MIS is responsible for managing the following in part or in whole.

1. IT Service Level Agreements (Expectations)
2. IT Service Capacity
3. IT Service Availability
4. IT Service Continuity
5. IT Information Security
6. IT-related Finance / Procurement

Whenever multiple incidents occur simultaneously, **prioritization should be based on both urgency and impact**. Unresolved high-priority incidents are to be reported to the management.

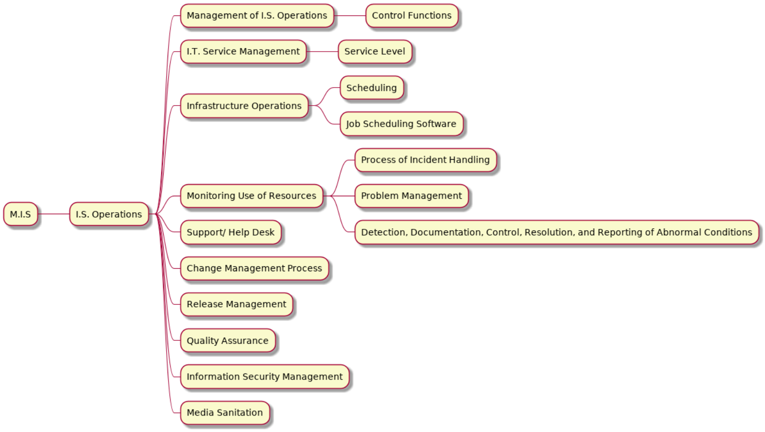
1.3. MIS and the Management

MIS and Management should agree on a reasonable Recovery Time Objective (RTO) and a reasonable Recovery Point Objective (RPO) for key IT services. This gives a target on how long a particular service can be down following a disaster. It also gives a target on the recency of the data that will be loaded once the service up after a disaster.

In general, the faster the recovery, the more costly and harder things are to be maintain. The more complete the data to be recovered, the more costly also. The right balance is normally achieved when there’s good understanding between MIS and the management.

2

Information Systems Operations


M.I.S
I.S. Operations
Management of I.S. Operations
Control Functions
I.T. Service Management
Service Level
Infrastructure Operations
Scheduling
Job Scheduling Software
Monitoring Use of Resources
Process of Incident Handling
Problem Management
Detection, Documentation, Control, Resolution, and Reporting of Abnormal Conditions
Support/ Help Desk
Change Management Process
Release Management
Quality Assurance
Information Security Management
Media Sanitation

2.1. Management of I.S. Operations

Tasks of the MIS staff include:

1. Execute and monitor scheduled jobs.
2. Facilitate timely backup.
3. Monitor unauthorized access and use of sensitive data.
4. Monitor and review the extent of adherence to IS operations procedures as established by IS and business management.
5. Participate in tests of disaster recovery plans (DRPs).
6. Monitor the performance, capacity, availability and failure of information resources.

7. Facilitate troubleshooting and incident handling.

The Procedure Documentation of MIS will include the following

1. Operations procedures that are based on operating instructions and job flows for computer and peripheral equipment• Procedures for monitoring systems and applications
2. Procedures for detecting systems and applications errors and problems
3. Procedures for handling IS problems and escalation of unresolved issues
4. Procedures for backup and recovery

2.1.1. Control Functions

2.2. I.T. Service Management

The fundamental premise associated with ITSM is that IT can be managed through a series of discrete processes that provide service to the business.

Service-level management is the process of defining, agreeing on, documenting and managing levels of service that are required and cost justified. Service-level management deals with more than the SLAs themselves; it includes the production and maintenance of the service catalog, service review meetings and service improvement plans (SIPs) for areas that are not achieving their SLAs.

2.2.1. Service Level Agreements

An SLA is an agreement between the IT organization and the customer. The SLA details the service(s) to be provided. The IT organization could be an internal IT department or an external IT service provider, and the customer is the business.

The SLA describes the services in nontechnical terms, from the viewpoint of the customer. During the term of the agreement, it serves as the standard for measuring and adjusting the services.

Defined service levels must be regularly monitored by an appropriate level of management to ensure that the objectives of IS operations are achieved. Monitoring of service levels is essential for outsourced services, particularly if the third party is involved in directly providing services to an organization’s customers.

It is important to note that when service delivery is outsourced, only responsibility for serviced provision is outsourced—accountability is not and still rests with the organization.

2.3. Infrastructure Operations

2.3.1. Scheduling

2.4. Monitoring Use of Resources

2.4.1. Process of Incident Handling

Incident management focuses on providing increased continuity of service by reducing or removing the adverse effect of disturbances to IT services and covers almost all nonstandard operations of IT services—thereby defining the scope to include any nonstandard event. In addition to initiation, other steps in the incident life cycle may include classification, assignment to specialists, resolution and closure.

For example, there could be a situation where a service request from the chief information officer (CIO) for a printer problem arrives at the same time as a request from the technology team to attend to a server crash. IS management should have parameters in place for assigning the priority of these incidents, considering both the urgency and impact.

Unresolved incidents are escalated based on the criteria set by IS management. Incident management is reactive, and its objective is to respond to and resolve issues restoring normal service (as defined by the SLA) as quickly as possible.

2.4.2. Problem Management

Problem management aims to resolve issues through the investigation and in-depth analysis of a major incident or several incidents that are similar in nature to identify the root cause. Standard methodologies for root cause analysis include the development of fishbone/Ishikawa cause-and-effect diagrams, brainstorming and the use of the 5 Whys—an iterative question-asking technique used to explore the cause-and-effect relationships underlying a problem.

After a problem is identified and analysis has identified a root cause, the condition becomes a \known error. A workaround can then be developed to address the error state and prevent future occurrences of the related incidents.

This problem is then added to the known error database (KEDB). The goal is to proactively prevent reoccurrence of the error elsewhere or, at a minimum, have a workaround that can be provided immediately should the incident reoccur.Problem management and incident management are related but have different methods and objectives. Problem management's objective is to reduce the number and/or severity of incidents, while incident management's objective is to return the affected business process back to its normal state as quickly as possible, minimizing the impact on the business. Effective problem management can show a significant improvement in the quality of service of an IS organization.

2.4.3. Detection, Documentation, Control, Resolution, and Reporting of Abnormal Conditions

Because of the highly complex nature of software, hardware and their interrelationships, a mechanism should exist to detect and document any abnormal conditions that could lead to the identification of an error.

For control purposes, the ability to add to the error log should not be restricted. The ability to update the error log, however, should be restricted to authorized individuals, and the updates should be traceable.

Problem escalation procedures generally include:

- Names/contact details of individuals who can deal with specific types of problems
- Types of problems that require urgent resolution
- Problems that can wait until normal working hours

Problem resolution should be communicated to the appropriate entities. This can be through an official email thread that discusses the problem straight up to its resolution.

2.5. Support/ Help Desk

Support is generally triaged when a help desk ticket/call is initiated and then escalated based on the complexity of the issue and the level of expertise required to resolve the problem.

The primary purpose of the help desk is to service the user. The second is to escalate issues it cannot resolve. The third is to document.

The basic function of the help desk is to be the first, single and central point of contact for users and to follow an incident management process.

2.6. Change Management Process

Change management is used when changing hardware, installing or upgrading to new releases of off-the-shelf applications, installing a software patch and configuringvarious network devices (e.g., firewalls, routers and switches).

The procedures associated with this process ensure that:

- All relevant personnel are informed of the change and when it is happening.
- System, operations and program documentation are complete, up to date and in compliance with the established standards.
- Job preparation, scheduling and operating instructions have been established.
- System and program test results have been reviewed and approved by user and project management.
- Data file conversion, if necessary, has occurred accurately and completely as evidenced by review and approval by user management.
- System conversion has occurred accurately and completely as evidenced by review and approval by user management.
- All aspects of jobs turned over have been tested, reviewed and approved by control/operations personnel.
- Legal or compliance aspects have been considered.
- The risk of adversely affecting the business operation are reviewed and a rollback plan is developed to back out the changes, if necessary.

Apart from change control, standardized methods and procedures for change management are needed to ensure and maintain agreed-on levels in quality service. These methods are aimed at minimizing the adverse impact of any probable incidents triggered by change that may arise.

This is achieved by formalizing and documenting the process of change request, authorization, testing, implementation and communication to the users. Change requests are often categorized into emergency changes, major changes and minor changes, and may have different change management procedures in place for each type of change.

2.7. Patch Management

Patch management is an area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system to maintain up-to-date software and often to address security risk.

Patches can be ineffective and can cause more problems than they fix. To avoid problems, patch management experts suggest that system administrators take simple steps, such as performing backups and testing patches on non- critical systems prior to installations.

2.8. Release Management

The term release is used to describe a collection of authorized changes. The release will typically consist of several problem fixes and enhancements to the service. The releases, whether major or minor, will have a unique identity.

The releases are controlled, and, if any problems arise in the new release, one should be able to back out completely and restore the system to its previous state. Suitable contingency plans may also be developed, if it is not completely restorable. These plans are developed before the new release is implemented.

The common types of releases are the following:

- Major Release
- Minor Release
- Emergency Release

Many new system implementations will involve phased delivery of functionality and thus require multiple releases. In addition, planned releases will offer an ongoing process for system enhancement.

Planning a release involves:

- Gain consensus on the release’s contents.
- Agree to the release strategy (e.g., the phasing over time and by geographical location, business unit and customers).
- Produce a high-level release schedule.
- Plan resource levels (including staff overtime).
- Agree on roles and responsibilities.
- Produce back-out plans.
- Develop a quality plan for the release.
- Plan acceptance of support groups and the customer

While change management is the process whereby all changes go through a robust testing and approval process, release management is the process of putting the software changes into production.

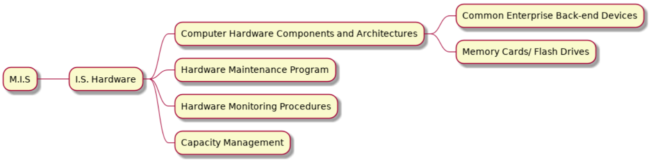
2.9. Quality Assurance

2.10. Information Security Management

2.11. Media Sanitation

3

Information Systems Hardware


M.I.S
I.S. Hardware
Computer Hardware Components and Architectures
Common Enterprise Back-end Devices
Memory Cards/ Flash Drives
Hardware Maintenance Program
Hardware Monitoring Procedures
Capacity Management

3.1. Computer Hardware Components and Architectures

3.1.1. Common Enterprise Back-end Devices

Following are some of the most common devices encountered:

Print servers

Businesses of all sizes require that printing capability be made available to users across multiple sites and domains. Generally, a network printer is configured based on where the printer is physically located and who within the organization needs to use it. Print servers allow businesses to consolidate printing resources for cost savings.

File servers

File servers provide for organizationwide access to files and programs. Document repositories can be centralized to a few locations within the organization and controlled with an access-control matrix. Group collaboration and document management are easier when adocument repository is used, rather than dispersed storage across multiple workstations.

Application (program) servers

Application servers typically host the software programs that provide application access to client computers, including processing the application business logic and communication with the application's database. Consolidation of applications and licenses in servers enables centralized management and a more secure environment.

Web servers

Web servers provide information and services to external customers and internal employees through web pages. They are normally accessed by their uniform resource locators (URLs).

Proxy servers

Proxy servers provide an intermediate link between users and resources. As opposed to direct access, proxy servers will access services on a user's behalf. Depending on the services being proxied, a proxy server may render more secure and faster response than direct access.

Database servers

Database servers store data and act as a repository. The servers concentrate on storing information rather than presenting it to be usable. Application servers and web servers use thedata stored in database servers and process the data into usable information.

Appliances (specialized devices)

Appliances provide a specific service and normally are not capable of running other services. As a result, the devices are significantly smaller and faster, and very efficient. Capacity and performance demands require certain services to be run on appliances instead of generic servers.

Examples of appliances are:

- Firewalls
- Intrusion detection systems (IDSs)
- Intrusion prevention systems (IPSs)
- Switches
- Routers

- Virtual private networks (VPNs)
- Load balancers

3.1.2. Memory Cards/ Flash Drives

Risks

Risk related to the use of USBs includes the following:

Viruses and other malicious software

USB drives present a vector for computer viruses that is very difficult to defend against. Whenever files are transferred between two machines, there is a risk that malware (e.g., viruses, spyware and keyloggers) will be transmitted, and USB drives are no exception. Some USB drives include a physical switch that can put the drive in read-only mode. When transferring files to an untrusted machine, a USB drive that is in read-only mode will prevent any data (including viruses) to be written to the device.

Data theft

Hackers, corporate spies and disgruntled employees steal data, and in many cases, these are crimes of opportunity. With a USB drive, any unattended and unlocked PC with a USB port provides an opportunity for criminal activity. Social engineering can give a hacker physical access to a corporate PC to steal data or plant spyware.

Data and media loss

The portability of USB drives presents an increased risk for lost data and media. If an unencrypted USB device is lost, any individual who finds the device will be able to access the data on the drive.

Corruption of data

If the drive is improperly unplugged, then data loss can occur due to corruption. USB drives differ from other types of removable media, such as CD-ROM and DVD- ROM devices, because the computer is not automatically alerted when USB drives are removed. Users of USB drives must alert the computer when they intend to remove the device; otherwise, the computer will be unable to perform the necessary clean-up functions required to disconnect the device, especially if files from the device are currently open.

Loss of confidentiality

Because of its convenient small physical size and large logical size, a significant amount of data can be stored on a USB drive. Some stored information is confidential, and loss of data becomes a risk when the drive is lost, increasing the risk of the data falling into the hands of a competitor. Legal issues can also be associated with loss of confidentiality. For example, in the United States, lost or compromised patient data can indicate a breach of patient privacy, thus violating the Health Insurance Portability and Accountability Act (HIPAA).

Security Control

The following controls can be used to help reduce risk associated with the use of USB devices:

Encryption

An ideal encryption strategy allows data to be stored on the USB drive but renders the data useless without the required encryption key, such as a strong password or biometric data. Products are available to implement strong encryption and comply with the latest Federal Information Processing Standards (FIPS). Encryption is a good method to protect information written to the device from loss or theft of the device. But unless the information is also encrypted on the network or local workstation hard drive, sensitive data still are exposed to theft.

The lock desktop policy enforcement

In higher-risk environments, desktop computers should be configured to automatically lock after short intervals.

Antivirus policy

Antivirus software should be configured to scan all attached drives and removable media. Users should be trained to scan files before opening them.

Inclusion of return information

If a USB drive is lost or misplaced, including a small, readable text file containing return information may help with device retrieval. It would be prudent to NOT include company details, but rather a phone number or post office box. It also would be prudent to include a legal disclaimer that clearly identifies the information on the drive as confidential and protected by law.

3.2. Hardware Maintenance Program

To ensure proper operation, hardware must be routinely cleaned and serviced.

Maintenance should be scheduled to closely coincide with vendor-provided specifications. Maintenance is also important for environmental hardware that controls temperature and humidity, fire protection and electrical power.

- Reputable service company information for each hardware resource requiring routine maintenance
- Maintenance schedule information
- Maintenance cost information
- Maintenance performance history information, such as planned versus unplanned, executed and exceptional

The IS Unit should monitor, identify and document any deviations from vendor maintenance specifications and provide supporting arguments for this deviation

3.3. Hardware Monitoring Procedures

The following are typical procedures and reports for monitoring the effective and efficient use of hardware:

Availability reports

These reports indicate the time periods during which the computer is in operation and available for use by users or other processes. A key concern addressed by this report is excessive IS unavailability, referred to as downtime. This unavailability may indicate inadequate hardware facilities, excessive OS maintenance, the need for preventive maintenance, inadequate environmental facilities (e.g., power supply or air conditioning) or inadequate training for operators.

Hardware error reports

These reports identify CPU, I/O, power and storage failures. These reports should be reviewed by IS operations management to ensure that equipment is functioning properly, to detect failures and to initiate corrective action. The MIS team should be aware that attribution of an error in hardware or software is not necessarily easy and immediate. Reports should be checked for intermittent or recurring problems, which might indicate difficulties in properly diagnosing the errors.

Asset management reports

These reports provide an inventory of network-connected equipment, such as PCs, servers, routers and other devices.

Utilization reports

These automated reports document the use of the machine and peripherals. Software monitors are used to capture utilization measurements for processors, channels and secondary storage media, such as disk and tape drives. Depending on the OS, resource utilization for multiuser computing environments found in mainframe/large-scale computers should average in the 85- to 95-percent range, with allowances for utilization occasionally reaching 100 percent and falling below 70 percent. Trends from utilization reports can be used by IS management to predict whether more or fewer processing resources are required.

3.4. Capacity Management

The following information is key to managing capacity.

- CPU utilization
- Computer storage utilization
- Internet Speed
- LAN and WAN bandwidth utilization
- I/O channel utilization
- Number of users
- New technologies
- New applications
- Service level agreements (SLAs)

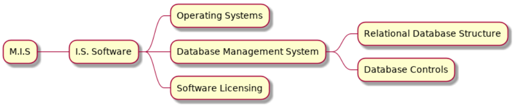
An element in capacity management is deciding whether to host the organization's applications distributed across several small servers, consolidated onto a few large servers, in the cloud or combinations of the three hosts. Consolidating applications on a few large servers (also known as application stacking) often allows the organization to make better overall use of the resources, but it increases the impact of a server outage, and it affects more applications when the server has to be shut down for maintenance.

Using the cloud allows extra capacity to be purchased on demand, but also brings the risk of relying on the supplier.

Capacity management must also include network devices, such as switches and routers, that comprise physically and logically separated networks (virtual local area networks [VLANs]).

4

I.S. Architecture and Software



5

Information System Architecture and Software

Organizations may use multiple service delivery channels, such as mobile apps, the Internet, service outlets, third-party service providers and automated kiosks. These channels use different technologies that may be serviced by the same backend database.

5.1. Operating Systems

It is common for OSs to run on virtual servers. In a virtual environment, software is used to partition one physical server into multiple independent virtual servers. Each of these environments can then run its own (and if required different) OS. To the operator, the OS behaves as if it were running on a physical server.

5.2. Database Management System

DBMS system software aids in organizing, controlling and using the data needed by application programs. A DBMS provides the facility to create and maintain a well-organized database.

The primary functions include the following.

- Reduced data redundancy
- Decreased access time
- Basic security over sensitive data

The DBMS can include a **data dictionary** that identifies the fields, their characteristics and their use. Active data dictionaries require entries for all data elements and assist application processing of data elements, such as providing validation characteristics or print formats. Passive dictionaries are only a repository of information that can be viewed or printed.

5.2.1. Relational Database Structure

The relational model is based on the set theory and relational calculations. A relational database allows the definition of data structures, storage/ retrieval operations and integrity constraints.

Data and relationships among data are organized in tables. A table is a collection of rows. A row is also known as a tuple. Each row in a table contains the same columns. Columns are also called Domains or Attributes. Columns correspond to fields. Tuples are equal to records in a conventional file structure.

Relational tables have the following properties:

- Values are atomic
- Each row is unique
- Column values are of the same kind
- The sequence of columns is significant
- The sequence of rows is insignificant
- Each column has a unique name

A key feature of relational databases is the use of **normalization** rules to minimize the amount of information needed in tables to satisfy the users' queries to the database.

Normalizations rules generally include the following.

1. A given instance of a data object has one and only one value for each attribute
2. Attributes represent elementary data items; they should have no internal structure

3. Each tuple has a primary key that identifies some entity. The rest of the attributes should be mutually independent of each other; thus making the tuple fully dependent on the primary key
4. Any foreign key should either be null or have a value linking to other tables; this is known as referential integrity.

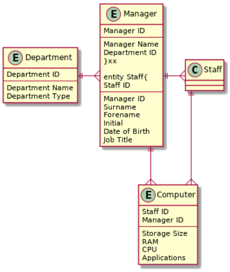


Figure 5.1. Example Relational Database Organization

- The sequence of columns is insignificant.
- The sequence of rows is insignificant.
- Each column has a unique name.

Certain fields may be designated as keys, so searches for specific values of that field will be quicker because of the use of indexing. If fields in two different tables take their values from the same set, a join operation can be performed to select related records in the two tables by matching values in those fields. This can be extended to joining multiple tables on multiple fields. These relationships are only specified at retrieval time, so relational databases are dynamic.

A key feature of relational databases is the use of normalization rules to minimize the amount of information needed in tables to satisfy the users' structured and unstructured queries to the database. Generally followed, normalization rules include:

- A given instance of a data object has only one value for each attribute.
- Attributes represent elementary data items; they should contain no internal structure.
- Each tuple (record) consists of a primary key that identifies some entity, together with a set of zero or more mutually independent attribute values that describes the entity in some way (fully dependent on primary key).

- Any foreign key should have a null value or should have an existing value linking to other tables; this is known as referential integrity.

5.2.2. Database Controls

It is critical that database integrity and availability are maintained. This is ensured through the following controls:

- Establish and enforce definition standards.
- Establish and implement data backup and recovery procedures to ensure database availability.
- Establish the necessary levels of access controls, including privileged access, for data items, tables and files to prevent inadvertent or unauthorized access.
- Establish controls to ensure that only authorized personnel can update the database.
- Follow database restructuring procedures when making logical, physical and procedural changes.
- Use database performance reporting tools to monitor and maintain database efficiency (e.g., available storage space, buffer size, CPU usage, disk storage configuration and deadlock conditions).
- Minimize the ability to use nonsystem tools or other utilities (i.e., those outside security control, to access the database).

5.3. Software Licensing

There are two different software licensing types: free and paid.

5.3.1. Free

Open source

The software may be used, copied, studied, modified and redistributed as required. Open source is usually accompanied by the program source and a copy of the software license (for example, the GNU General Public License). A well-known example is Linux.

Freeware

The software is free, but the source code cannot be redistributed. A well-known example is Adobe Acrobat Reader®.

Shareware

The software may be free initially; however, this may only be on a trial basis or have limited functionality compared to the full, commercial version (may also be known as trial version, demo ware or an evaluation copy).

5.3.2. Paid

Per central processing unit

Depends on the power of the server, specifically the number of the (CPU) CPUs; could include the number of CPU cores

Per seat

Depends on the number of unique users of the system

Concurrent users

Depends on the total number of users using the software within a predefined period of time

Utilization

Depends on how busy the CPU is or the number of users that are active at any one time

Per workstation

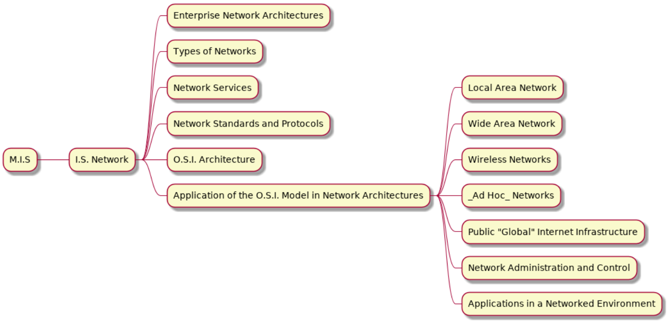
Depends on the number of individual workstations (NOT users) that connect to the software

Enterprise

Everyone from the company may use.

6

I.S. Network Infrastructure


M.I.S
I.S. Network
Enterprise Network Architectures
Types of Networks
Network Services
Network Standards and Protocols
O.S.I. Architecture
Application of the O.S.I. Model in Network Architectures
Local Area Network
Wide Area Network
Wireless Networks
Ad Hoc Networks
Public "Global" Internet Infrastructure
Network Administration and Control
Applications in a Networked Environment

7

I.S. Network Infrastructure

7.1. Enterprise Network Architectures
7.2. Types of Networks
7.3. Network Services
7.4. Network Standards and Protocols
7.5. O.S.I. Architecture
7.6. Application of the O.S.I. Model in Network Architectures
7.6.1. Local Area Network
L.A.N. Design Fundamentals and Specifications
Network Physical Media Specifications
Implementation of W.A.N.s
L.A.N. Topologies and Protocols
L.A.N. Media Access Technologies
L.A.N. Components
L.A.N. Technology Selection Criteria
7.6.2. Wide Area Network
W.A.N. Message Transmission Techniques
W.A.N. Devices
W.A.N. Technologies
7.6.3. Wireless Networks
Wireless Wide Area Networks
Wireless Local Area Networks
Wired Equivalent Privacy adn Wi-Fi Protected Access (WPA/WPA 2)
Wireless Personal Area Networks
7.6.4. Ad Hoc Networks
Wireless Apllication Protocol
7.6.5. Public "Global" Internet Infrastructure
TCP/IP and its Relation to the OSI Reference Model
TCP/IP Internet World Wide Web Services
General Internet Terminology
Transborder Data Flow
7.6.6. Network Administration and Control
Network Performance Metrics
Network Management Issues
Network Management Tools

The tools consist of reports, monitors and analyzers.

Response time reports

identify the time necessary for a command entered by a user at a terminal to be answered by the host system. Response time is important because end users experiencing slow response time will be reluctant to utilize IS resources to their fullest extent. These reports typically identify average, worst and best response times over a given time interval for individual telecommunication lines or systems. These reports should be reviewed by IS management and system support personnel to track potential problems. If response time is slow, all possible causes, such as I/O channel bottlenecks, bandwidth utilization and CPU capacity, should be investigated; various solutions should be analyzed; and an appropriate and cost-justified corrective action should be taken.

Downtime reports

track the availability of telecommunication lines and circuits. Interruptions due to power/line failure, traffic overload, operator error or other anomalous conditions are identified in a downtime report.

If downtime is excessive, IS management should consider the following remedies:

- Add or replace telecommunications lines.
- Switch to a more dependable transmission link (such as dedicated lines versus shared lines).
- Install backup power supplies.• Improve access controls.
- Closely monitor line utilization to better forecast user needs, both in the near and long term.

Help desk reports

are prepared by the help desk, which is staffed or supported by IT technicians who are trained to handle problems occurring during normal IS usage. If an end user encounters any problem, he/she can contact the help desk for assistance. Help desk facilities are critical to the telecommunication environment since they provide end users with an easy means of identifying and resolving problems quickly, before they have a major impact on IS performance and end-user resource utilization. Reports prepared by the help desk provide a history of the problems and their resolution.

Online monitors

check data transmission accuracy and errors. Monitoring can be performed by echo checking (received data are bounced back to sender for verification) and status checking all transmissions, ensuring that messages are not lost or transmitted more than once. Network monitors provide a real time display of network nodes and status.

Network (protocol) analyzers

are diagnostic tools attached to a network link that use network protocols' intelligence for monitoring the packets flowing along the link and produce network usage reports. Network analyzers are typically hardware-based and operate at the data link and/or network level.

Output includes the following information:

- Protocol(s) in use
- Type of packets flowing along the monitored link
- Traffic volume analysis
- Hardware errors, noise and software problems
- Other performance statistics (e.g., percentage of used bandwidth)
- Problems and possible solutions

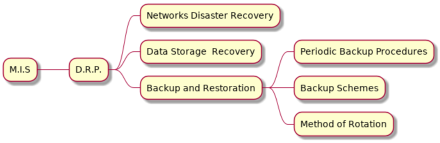
7.6.7. Applications in a Networked Environment

Client-Serve Technology

Middleware

8

Disaster Recovery Planning



We have to be able to list and classify our systems.

Critical

These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced by manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.

Vital

These functions can be performed manually, but only for a brief period of time. There is a higher tolerance to interruption than with critical systems and, therefore, somewhat lower costs of interruption, provided that functions are restored within a certain time frame (usually five days or less).

Sensitive

These functions can be performed manually, at a tolerable cost and for an extended period of time.While they can be performed manually, it usually is a difficult process and requires additional staff to perform.

Nonsensitive

These functions may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.

For each classification, we determine a Recovery Point Objective (RPO) and a corresponding Recovery Time Objective (RTO). There should be common understanding between the management and the MIS regarding these expectations and commitments.

Having a RPO and a RTO allows us to explore alternatives and then select stratigies. Different alternatives may require different man-power, hardware, and contractual needs.

8.1. Telecommunication Networks Disaster Recovery Methods

Uninterruptible power supplies (UPSs) should be sufficient to provide backup to the telecommunication equipment as well as the computer equipment.

Methods for network protection are:

Redundancy—This involves a variety of solutions, including:

- Providing extra capacity with a plan to use the surplus capacity if the normal primary transmission capability is not available. For a LAN, a second cable can be installed through an alternate route for use if the primary cable is damaged.
- Providing multiple paths between routers
- Using dynamic routing protocols, such as Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP)
- Providing for failover devices to avoid single point of failures in routers, switches, firewalls, etc.
- Saving configuration files for recovery if network devices, such as those for routers and switches, fail. For example, organizations should use Trivial File Transport Protocol (TFTP) servers. Most network devices support TFTP for saving and retrieving configuration information.

8.2. Data Storage Disaster Recovery

For on-premise installations, it’s the redundancies in the server hard drives that is best for keeping the data available during storage failure.

For the cloud, volume backups are best.

Redundant Array of Independent (or Inexpensive) Disks (RAID) is the most common, basic way to protect data against a single point of failure, in this instance, a disk failure. RAID provides performance improvements and fault-tolerant capabilities via hardware or software solutions, breaking up data and writing data to a series of multiple disks to simultaneously improve performance and/or save large files. These systems provide the potential for cost-effective mirroring offsite for data backup. A variety of methods, categorized into 11 levels (the most popular being 0 [stripe], 1 [mirror], their combinations [0+1 or 1+0] and 5), is defined for combining several disk drives into what appears to the system as a single disk drive. RAID improves on the single-drive-only solution, because it offers better performance and/or data redundancy.

The array-based (hardware) replication is absolutely transparent to the application (i.e., no special provisions are needed from the OS or the application side). If there is no disk array, the data stored on local server volumes (RAID or not) can still be replicated to a remote site by using host-based data replication solutions. These act similarly to hardware-based solutions.

8.3. Backup and Restoration

An inventory of contents at the offsite storage location should be maintained.

8.3.1. Periodic Backup Procedures

Scheduling the periodic backups can often be easily accomplished via an automated backup/media management system and automated job scheduling software. Using the integrated solution for backup/recovery procedures and media management will prevent erroneous or missed backup cycles due to operator error.

8.3.2. Backup Schemes

There are three main schemes for backup: full, incremental and differential. Each one has its advantages and disadvantages. Usually, the methods are combined, in order to complement each other.

Full Backup

This type of backup scheme copies all files and folders to the backup media, creating one backup set (with one or more media, depending on media capacity). The main advantage is having a unique repository in case of restoration, but it requires more time and media capacity.

Incremental Backup

An incremental backup copies the files and folders that changed or are new since the last incremental or full backup. If you have a full backup on day 1, your incremental backup on day 2 will copy only the changes from day 1 to day 2. On day 3, it will copy only the changes from day 2 to day 3, and so on. Incremental backup is a faster method of backup and requires less media capacity, but it requires that all backup sets restore all changes since a full backup.

	Day 1	Day 2	Day 3	Day 4	Day 5	Day 6	Day 7
File 1	x	x					
File 2	x		x				
File 3	x			x			
File 4	x				x		

Differential Backup

A differential backup copies all files and folders that have been added or changed since a full backup was performed. This type of backup is faster and requires less media capacity than a full backup and requires only the last full and differential backup sets to make a full restoration. It also requires less time to restore than incremental backups, but it is slower and requires more media capacity than incremental backups because data that are backed up are cumulative.

	Day 1	**Day 2**	**Day 3**	**Day 4**	**Day 5**	**Day 6**	**Day 7**
File 1	x	x	x	x	x		
File 2	x		x	x	x		
File 3	x			x	x		
File 4	x				x		

8.3.3. Method of Rotation

Although there are various approaches for the rotation of media, one of the more accepted techniques is referred to as the Grandfather-Father-Son method. In this method, daily backups (son) are made over the course of a week. The final backup taken during the week becomes the backup for that week (father). The earlier daily backup media are then rotated for reuse as backup media for the second week. At the end of the month, the final weekly backup is retained as the backup for that month (grandfather). Earlier weekly backup media are then rotated for reuse in subsequent months. At the end of the year, the final monthly backup becomes the yearly backup. Normally, monthly and annual tapes/other media are retained and not subject to the rotation cycle.

	Mon	**Tues**	**Wed**	**Thurs**	**Fri**
week 1	son	son	son	son	father
week 2	son	son	son	son	father
week 3	son	son	son	son	father
week 4	son	son	son	son	grandfather

Testing all aspects of the DRP is the most important factor in achieving success in an emergency situation. The main objective of testing is to ensure that executing the plans will result in the successful recovery of the infrastructure and critical business processes. Testing should focus on:

- Identifying gaps
- Verifying assumptions
- Testing time lines
- Effectiveness of strategies
- Performance of personnel
- Accuracy and currency of plan information

Testing promotes collaboration and coordination among teams and is a useful training tool. Many organizations require complete testing annually. In addition, testing should be considered on the completion or major revision of each draft plan or complementary plans and following changes in key personnel, technology or the business/regulatory environment. Testing must be carefully planned and controlled to avoid placing the business at increased risk.