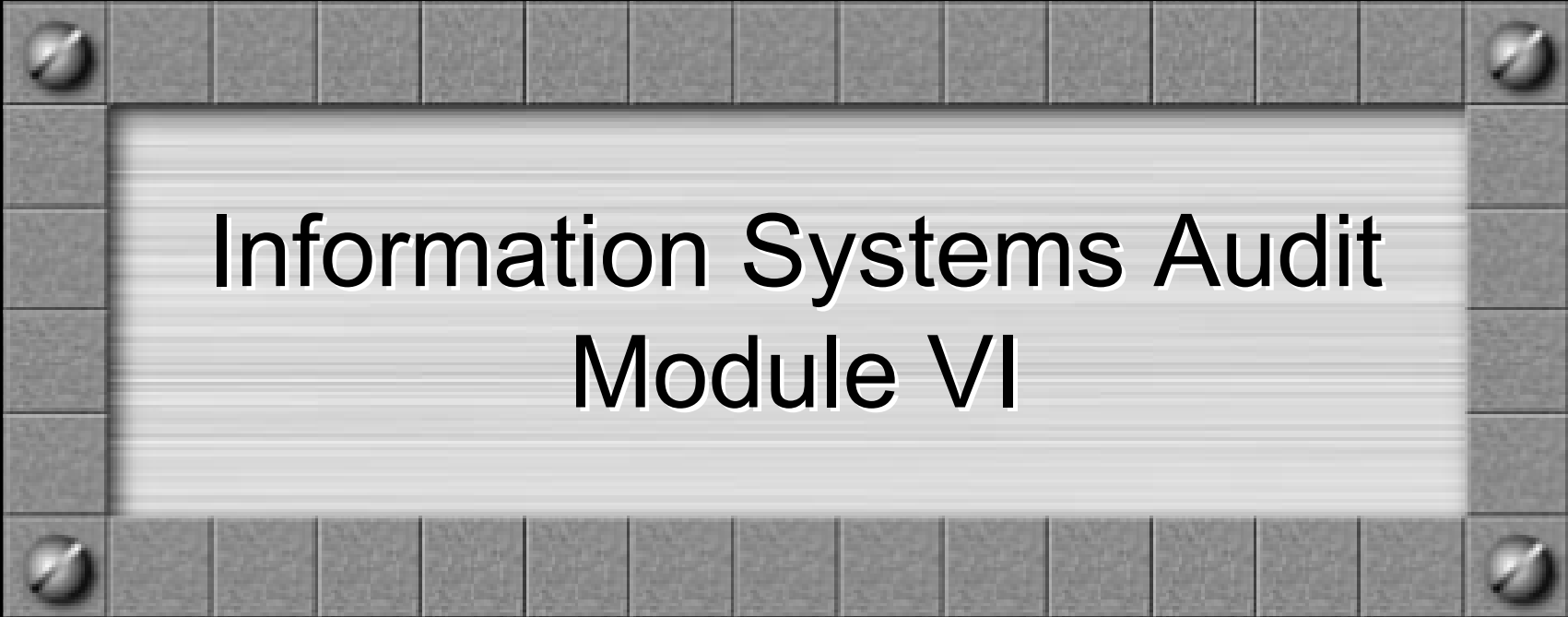




Information Systems Audit Module VI

Mathew A Thomas

Grad. CWA, FCA, MCA, CDM, ISA, CISSP.

Introduction

- ✓ About the Course
- ✓ About the Module
 - ▶ Module 6 (10%) 20 Questions
- ✓ About the Material
 - ▶ Source, Organisation
 - ▶ Module 6: Chapter 27

About this Presentation

- ✓ Chapter 27:
 - ▶ Business Continuity Planning 130
- ✓ Chapter 27:
 - ▶ Application Systems 153

Steps in Business Continuity Planning

- ✓ Initiate
- ✓ Perform Risk Assessment
- ✓ Choose Recovery Strategy
- ✓ Test and Validate

Initiate

- ✓ Establish a business continuity plan work group and develop a high-level business continuity planning strategy.
- ✓ Develop master schedule and milestones
- ✓ Obtain management support.

Perform Risk Assessment

- ✓ Perform a Risk Assessment exercise to identify threats and exposures to each of the core business processes.

Choose Recovery Strategy

- ✓ Identify Recovery strategy.
- ✓ Define notification procedures
- ✓ Procedures activating contingency plans
- ✓ Establish business recovery teams for each core business process.

Test and Validate

- ✓ Validate the company's business continuity plans.
- ✓ Develop and document contingency test plans.
- ✓ Prepare and execute tests.
- ✓ Update disaster recovery plans and procedures.

Disaster Events

- ✓ A disaster can be defined as unplanned interruptions of normal business process.
- ✓ Classification
 - ✦ Natural disasters
 - ▶ earthquakes, floods, wildfires, landslides, sleet and ice storms, high winds, tornados, and hurricanes
 - ✦ Technological disasters

Disaster Recovery Plan

- ✓ Emergency Plan
- ✓ Backup Plan
- ✓ Recovery Plan
- ✓ Test Plan

Emergency Plan

- ✓ Who is to be notified in the event of a disaster
- ✓ Actions to be taken within the installation
 - ✦ Shutdown systems, removal of files, power termination.
- ✓ Evacuation Procedures
- ✓ Return and Restart Procedures

Backup Plan

- ✓ Location of Back up Resources
- ✓ Site Assembly and Resumption
- ✓ Personnel
- ✓ Priorities while recovering
- ✓ Time frame for recovery

Recovery Plan

- ✓ To restore the installation to its full capability.
- ✓ Identification of Recovery team
- ✓ Provide Guidelines on priorities to be followed.
- ✓ Difficult for the plan to be specific
- ✓ Periodically review the responsibilities assigned to the team

Test Plan

- ✓ To identify deficiencies in the
 - ✦ emergency, backup and recovery plans.
 - ✦ Vigilance of organization and its personnel
- ✓ Test of Plans usually disrupts normal operations.

Risk Assessment/Analysis

- ✓ Basic Elements of the Risk Assessment Process
- ✓ Objectives of Risk Ranking
- ✓ Challenges Associated with Assessing Information Security Risks
- ✓ Risk Assessment Process
- ✓ Planning and Preparation
- ✓ Team Risk Assessment Activities
- ✓ Reporting
- ✓ Risk Ranking

Elements of the Risk Assessment Process

- ✓ Identify threats.
- ✓ Estimating the probability of each threat
- ✓ Identify and rank the value, sensitivity, and criticality of the operations and assets that could be affected should a threat materialize Estimate the potential losses or damage that could occur if a threat materializes.
- ✓ Identifying cost-effective actions to mitigate or reduce the risk.
- ✓ Document results and Develop an action plan.
- ✓ $ALE = SLE \times ARO$

Objectives of Risk Ranking

✓ Criticality Prioritization

- ✦ Identify business functions or processes and their associated resource requirements.
- ✦ Prioritize business processes according to time-sensitivity and criticality.

✓ Critical recovery time period (RTO, MTD)

- ✦ The critical recovery time period is the maximum amount of time allowed for the recovery of the of the business function.
- ✦ Time period is contingent upon the length of the disruption, the time of the day or month an interruption occurs.

Challenges In with Assessing InfoSec Risks

- ✓ Data are limited on risk factors
 - ✦ Likelihood of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses;
- ✓ Costs are inherently difficult to quantify
 - ✦ Loss of customer confidence
- ✓ Indirect costs
 - ✦ Possible loss of productivity that may result when new controls are implemented
- ✓ Information gets out of date due to changes in technology and factors such as improvements in tools available to would-be intruders.

Risk Assessment Process

Planning And Preparation Phase

Develop Project Plan and Select Assessment Team

Risk Management Coordinator and Business Manager

Team Risk Assessment Activities

Gather Information

Team Members and other Knowledgeable Individuals

Identify Threats

Corporate Threat Assessment Unit or
Team Members

Evaluate Assets and Threats

Team Members

Develop Scenarios

Team Members

Rank Scenario Risk

Team Members

Identify Countermeasures to
Mitigate Risk

Team Members and Business Unit



Risk Assessment Process

Reporting and Follow-up



Planning and Preparation

- ✓ Risk assessment execution plan developed
 - ✦ Designated Central coordinator
 - ✦ Senior managers
- ✓ This plan covers assessment objectives and methodology, team size and composition, and information requirements for conducting the assessment.
- ✓ Usually composed employees, and may include consultants.

Team Risk Assessment Activities

- ✓ Collect and analyse data on threats and potential vulnerabilities
- ✓ Process
 - ✦ Conduct interviews with the knowledgeable individuals
 - ✦ Once the interviews are completed, the team begins to analyze the information collected during the interviews to develop scenarios of possible undesired and damaging events.
- ✓ Consider how current organizational procedures or applications may compromise the organization's information resources.
- ✓ Rank scenarios according to how severe the effects of their damage or loss would be.
- ✓ Recommend corrective actions to reduce or mitigate risks

Reporting

- ✓ Exit briefing
 - ▶ Discuss the assessment findings with the management
 - ▶ High-risk scenario which may require immediate action
- ✓ Central coordinator then prepares a draft report, using a standard format, and distributes the report to team members for comment.
- ✓ Company develops an action plan for implementing the report recommendations.
- ✓ If Company decides does not to implement a recommendation the management must document their reasons for doing so.

Risk Ranking

✓ Tolerance

- ✦ The ability of a company to cope with the interruption of a business process determines the **tolerance** to the business process.
- ✦ In practice, tolerance is usually expressed as a monetary amount – the cost to the company if the business process is interrupted for a given unit of time.
- ✦ Cost of interruption is inversely related to the tolerance.

✓ Classification

- ✦ Critical
- ✦ Vital
- ✦ Sensitive
- ✦ Non-Critical

Critical

- ✓ Critical applications cannot be replaced by manual methods.
- ✓ Tolerance to interruption is very low
- ✓ Cost of interruption is very high
- ✓ Company would need to arrange to have access to hardware comparable to its own, and in the event of an emergency, plan to transfer the function to the backup hardware to resume processing.

Vital

- ✓ Can be performed manually but only for a brief period of time
- ✓ There is higher tolerance to interruption than with critical systems
- ✓ Can withstand a brief suspension of operations but cannot withstand an extended period of downtime.

Sensitive

- ✓ Can be performed manually, at tolerable cost, for an extended period of time.
- ✓ Can be performed manually with some difficulty
- ✓ May require additional staff to perform

Non-critical

- ✓ May be interrupted for an extended period of time, at little or no cost to the company
- ✓ Very little time is required to restore the data to a current or usable form

Other Components of an Effective BCP

- ✓ Notification Directory
- ✓ Insurance

Notification Directory

- ✓ A business continuity plan often contains a notification directory of persons to be notified in the event of a disaster.
 - ✦ The critical contact persons, who are often the team leaders. These team leaders in turn will call on their team members.
 - ✦ Equipment and software vendors.
 - ✦ Companies that have been designated to provide supplies and equipment or services.
 - ✦ Recovery facilities (including hot site representatives or predefined network communications rerouting services).
 - ✦ Off-site media storage facilities and persons within the company who are authorized to retrieve media from the off-site facility.
 - ✦ The insurance company.
 - ✦ Company providing contract personnel services.
- ✓ Notification Tree

Insurance

- ✓ Equipment and Facility Insurance
- ✓ Business interruption insurance
- ✓ Extra Expense
- ✓ Professional Liability (Errors & Omissions)
- ✓ Extra Equipment Coverage
- ✓ Data Reconstruction
- ✓ Specialized Equipment Coverage
- ✓ Valuable Papers and Records
- ✓ Fidelity Coverage
- ✓ Civil Authority
- ✓ Media Transit

Data Recovery Plan

✓ Classification of Data

- ✦ Critical, Vital, Sensitive, Noncritical

✓ Backup Strategies

✦ Traditional Backup to tape

- ★ Regular data backup to magnetic tape using backup/restore software and the removal of backups to off-site storage

✦ Electronic Vaulting

- ★ A WAN connection is established between the company facility and a remote tape library using high-bandwidth interconnection.

✦ Remote Mirroring

- ★ Perform duplicate writes to disks on identical (or at least similar) disk array platforms located some distance from the company facility far enough away so that the mirrored array is not affected by the same disaster that affects the primary or production array.

Alternatives for System Recovery

- ✓ Mirror site/Active Recovery Site
- ✓ Hot Site
- ✓ Warm Site
- ✓ Cold site
- ✓ Service Bureaus/Application Service Providers (ASPs)
- ✓ Reciprocal Backup Agreement

Mirror site/Active Recovery Site

- ✓ This is the most reliable and the most expensive method of systems recovery.
- ✓ Fully redundant systems called an active recovery site or a mirror site.
- ✓ Build and equip two identical data centres, those companies that can afford to do so have the ability to recover from almost any disaster.
- ✓ In the event of a disaster, redundant systems at a separate facility – which must be far enough so as not to have been affected by the same disaster – are brought on-line.

Hot Sites

- ✓ Fully configured and ready to operate within several hours
- ✓ Equipment and systems software must be compatible with the primary installation being backed up
- ✓ Additional needs are staff, programs, data files and documentation
- ✓ Own dedicated hot site or provided by another commercial organisation

Warm Sites

- ✓ Partially configured, usually with network connections and selected peripheral equipment, such as disk drives, tape drives and controllers, but without the main computer
- ✓ Or a Less powerful system CPU than the one generally used.

Cold Sites

- ✓ Only the basic environment (electrical wiring, air conditioning, flooring, etc.) to operate an information processing facility
- ✓ Activation of the site may take several weeks
- ✓ Company-owned cold site OR commercial cold site

Service Bureau / (ASPs)

✓ Service Bureau

- ✦ Contracting with a service bureau for emergency processing services
- ✦ Vendor of a banking application used by banking companies may offer a "service bureau" capability for the application.
- ✦ Vendor service bureaus are typically application-specific.
- ✦ They may not be suitable for an organisation that has several critical applications from different vendors.

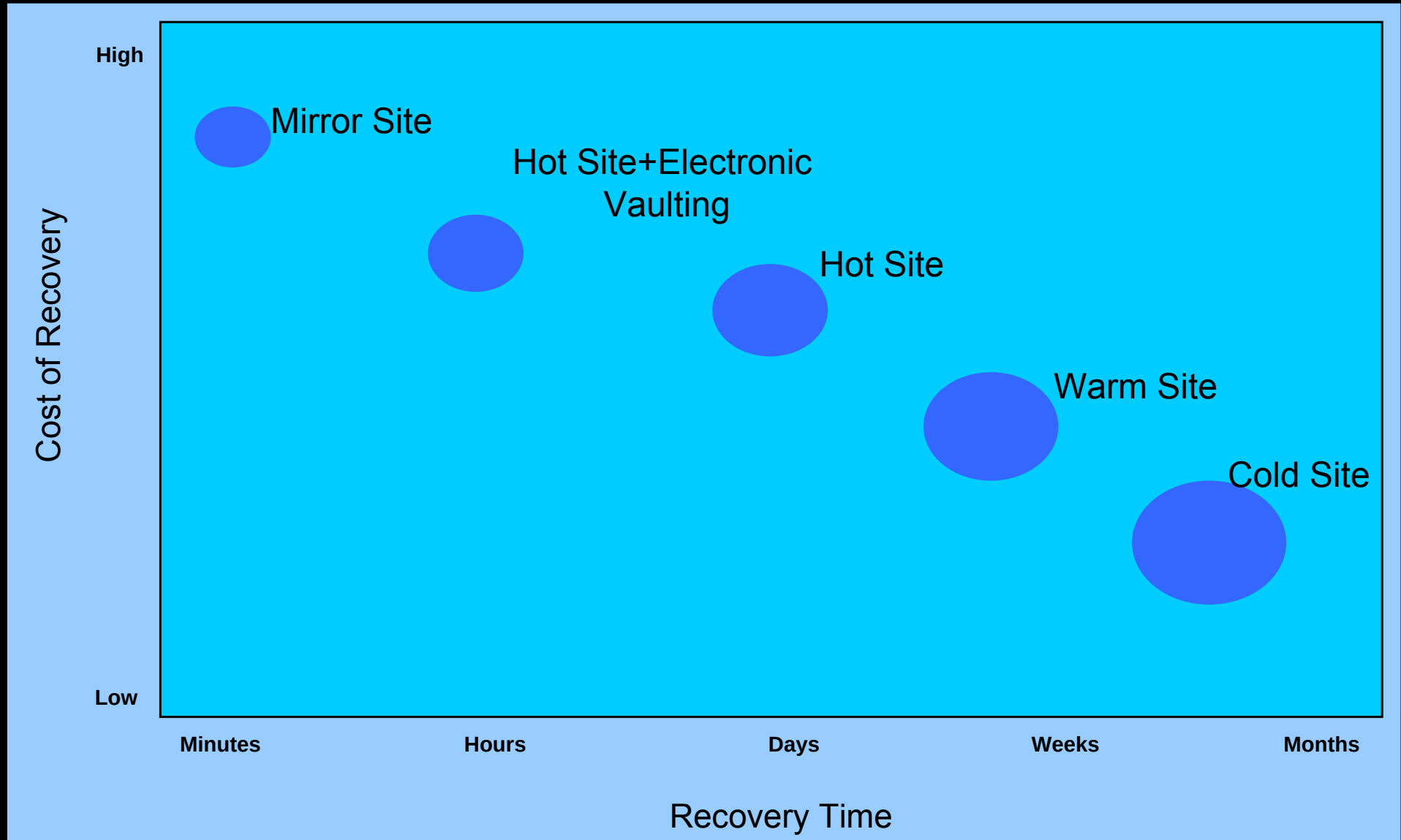
✓ ASP

- ✦ Provides a wider range of services than a service bureau. Example, Oracle.

Reciprocal Agreements

- ✓ Agreements between two or more organizations with similar equipment or applications
- ✓ Participants promise to provide computer time to each other when an emergency arises
- ✓ Low cost

Alternatives for System Recovery



Telecommunication Networks

- ✓ Redundancy
- ✓ Alternative Routing
- ✓ Diverse Routing
- ✓ Long Distance Network Diversity
- ✓ "Last Mile" Circuit Protection
- ✓ Voice Recovery

Redundancy

- ✓ Having extra capacity
- ✓ Use the surplus capacity when the normal primary transmission capability is not available.

Alternative Routing

- ✓ Route information via an alternate medium or path such as copper cable or fiber optics.
- ✓ Use of different networks, circuits or end points.
- ✓ Examples:
 - ✦ Dial-up circuits as an alternative to dedicated circuits
 - ✦ Cellular phones and microwave communication as an alternative to land circuits
 - ✦ Couriers as an alternative to electronic transmissions

Diverse Routing

- ✓ Diverse Routing uses circuits serving the same end points but routed over geographically separate transmission facilities.
- ✓ Route traffic through split cable facilities or duplicate cable facilities
- ✓ Different and or duplicate cable sheaths

Long Haul Network Diversity

- ✓ Recovery facilities vendors have provided diverse long-distance network availability utilizing T1 circuits among the major long-distance carriers.
- ✓ Ensures long-distance access should any one carrier experience a network failure

Last Mile Circuit Protection

- ✓ Redundant combination of local carrier T1 system, microwave and/or coaxial cable access to the local communications loop.
- ✓ Enables the facility to have access during a local carrier communication disaster.

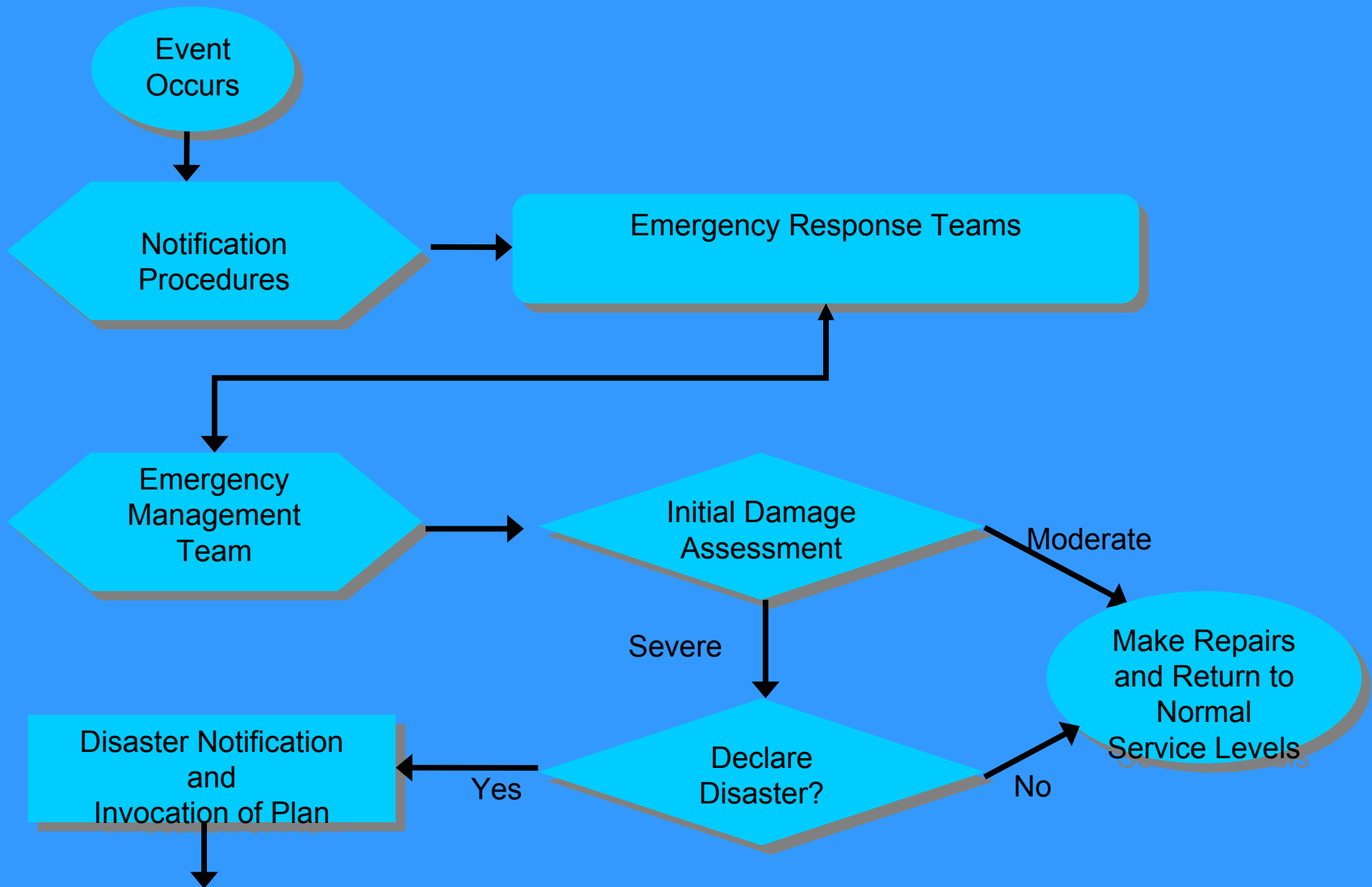
Voice Recovery

- ✓ Redundant cabling and alternative routing should also be provided for voice communication lines.
- ✓ Take into account PBX (private Branch Exchange) failures
- ✓ Backup PBX firmware.

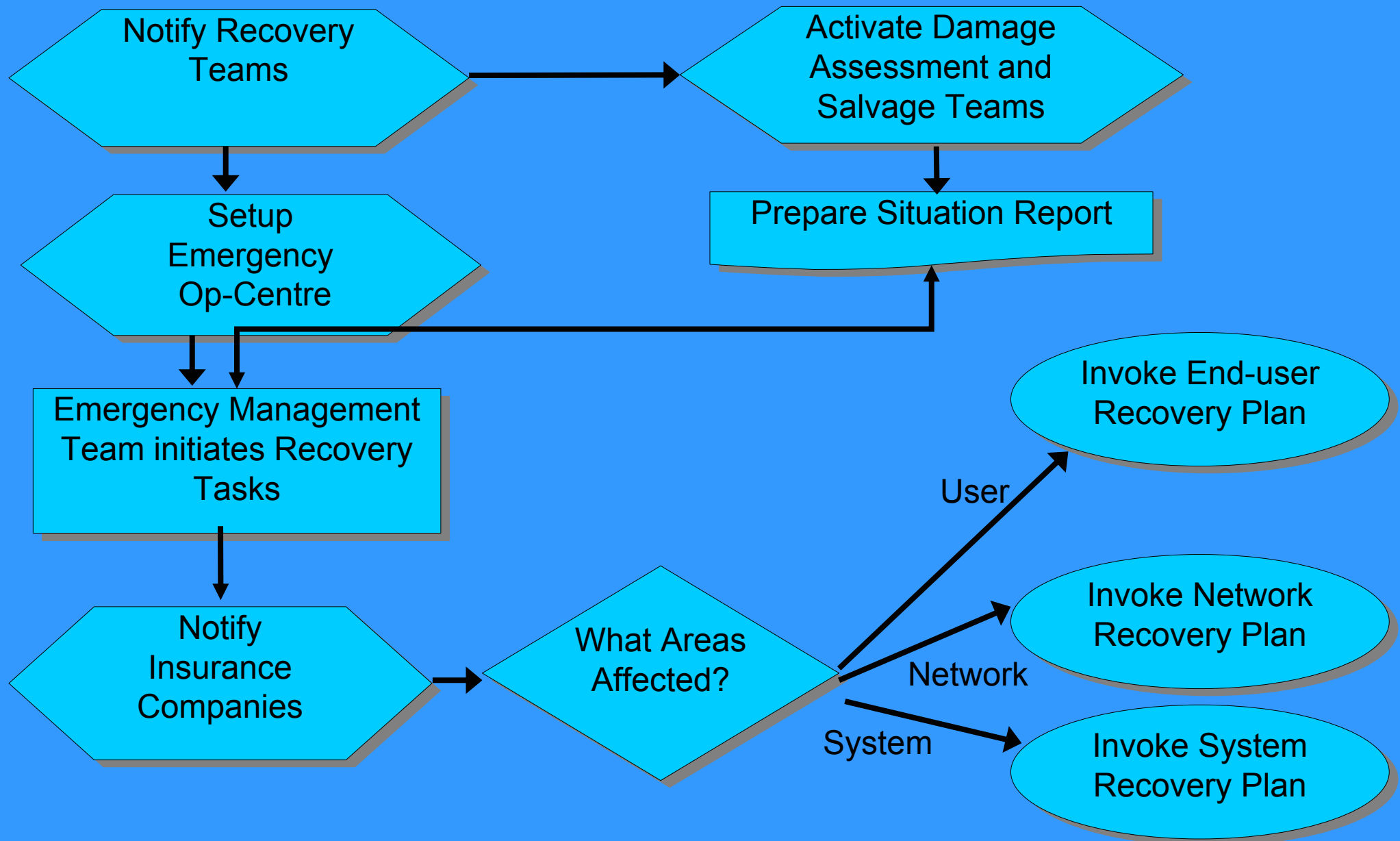
Continuity Plan Organization and Implementation

- ✓ Components of a Business Continuity Plan:
 - ✦ General information
 - ✦ Administrative Procedures
 - ✦ Operational Continuity Procedures
 - ✦ Information Systems Recovery Procedures
 - ✦ Application Resumption Plan

BCP Organizational Structure



BCP Organizational Structure



BCP Testing and Validation

- ✓ The objectives of testing
 - ✦ Testing as an audit tool
 - ✦ Testing as benchmarking
 - ✦ Testing as rehearsal
- ✓ The phases of testing
 - ✦ Pre-Test
 - ✦ Test
 - ✦ Post-Test

Objectives of testing

- ✓ Testing as an audit tool.
 - ✦ Verify completeness and accuracy of BCP
 - ✦ Evaluate the efficiency of the plan and to reveal its shortcomings.
- ✓ Testing as benchmarking
 - ✦ Measure performance of the recovery capability
 - ✦ Benchmark how quickly, under optimal conditions, recovery can be reasonably expected to occur following plan activation.
 - ✦ Actual level of service that is likely to be provided from the alternate site.
- ✓ Testing as rehearsal.
 - ✦ Training for team members

Phases of testing

- ✓ Pre-Test
 - Preparatory phase that lays the groundwork for the actual test
 - Not be carried out during an actual disaster
- ✓ Test
 - Operational activities are performed to test plan objectives
 - Move personnel, equipment and supplies to the recovery site
 - Execute various information processing tasks from there.
 - Actions are monitored and evaluated by properly trained and equipped staff members.
- ✓ Post-Test
 - All resources are restored to their original location
 - Delete data from third-party systems, restoring equipment and personnel to their normal locations
 - Formal evaluation of the plan
 - Suggest and implement improvements

The Types of Tests

- ✓ Checklist
- ✓ Structured walk-through
- ✓ Simulation
- ✓ Parallel
- ✓ Full-interruption

Checklist

- ✓ Copies of the plan are distributed to each of the teams.
- ✓ Each response team meets to review its response procedures to ensure that all information is current.

Structured Walk-through

- ✓ The response team members should meet to walk-through each step of their resumption procedures.
- ✓ Evaluate the effectiveness of each continuation activity and identify gaps, bottlenecks or other weakness in the plan.

Simulation

- ✓ A disruptive event is simulated without impacting normal operations.
- ✓ Validates
 - ▶ Notification procedures
 - ▶ Backup power systems
 - ▶ Hardware backup systems
 - ▶ Transportation arrangements
 - ▶ Alternate communication systems
 - ▶ Software and data backup systems
 - ▶ Alternate site processing
- ✓ The simulation may extend to actually relocating to the backup site and enacting recovery procedures but usually does not involve actual recovery process or alternate processing.

Parallel

- ✓ Full test of the plan utilizing all material and human resources
- ✓ Normal operations are not interrupted
- ✓ Processing is done at both the primary and alternate location.
- ✓ To ensure that critical systems will actually run at the alternate processing backup site
- ✓ Systems and personnel are relocated and the results of processing at both locations are compared.

Full-interruption

- ✓ Activating the complete business continuity plan
- ✓ Mobilization of personnel and resources to an alternate site after interrupting normal operations
- ✓ As far as BCP testing is concerned, this is the disaster.
- ✓ Very costly and should be used and scheduled with extreme caution.
- ✓ Best way to test a business continuity plan.

Business Continuity Plan Maintenance

- ✓ Business continuity plans lose their utility very quickly, often within a year or less
 - ✦ Staff have changed, vendors are different and resource requirements have changed.
 - ✦ Changes in business priorities will result in changes to critical business functions.
- Technological developments may result in drastic changes to hardware or software environments, which render a plan obsolete.
- ✓ If not maintained, the plan will have to be written from scratch within a few years.

Audit and Evaluation Techniques for BCP

- ✓ Priorities
- ✓ Strategies
- ✓ Responsibilities and Tasks

BCP Audit: Priorities

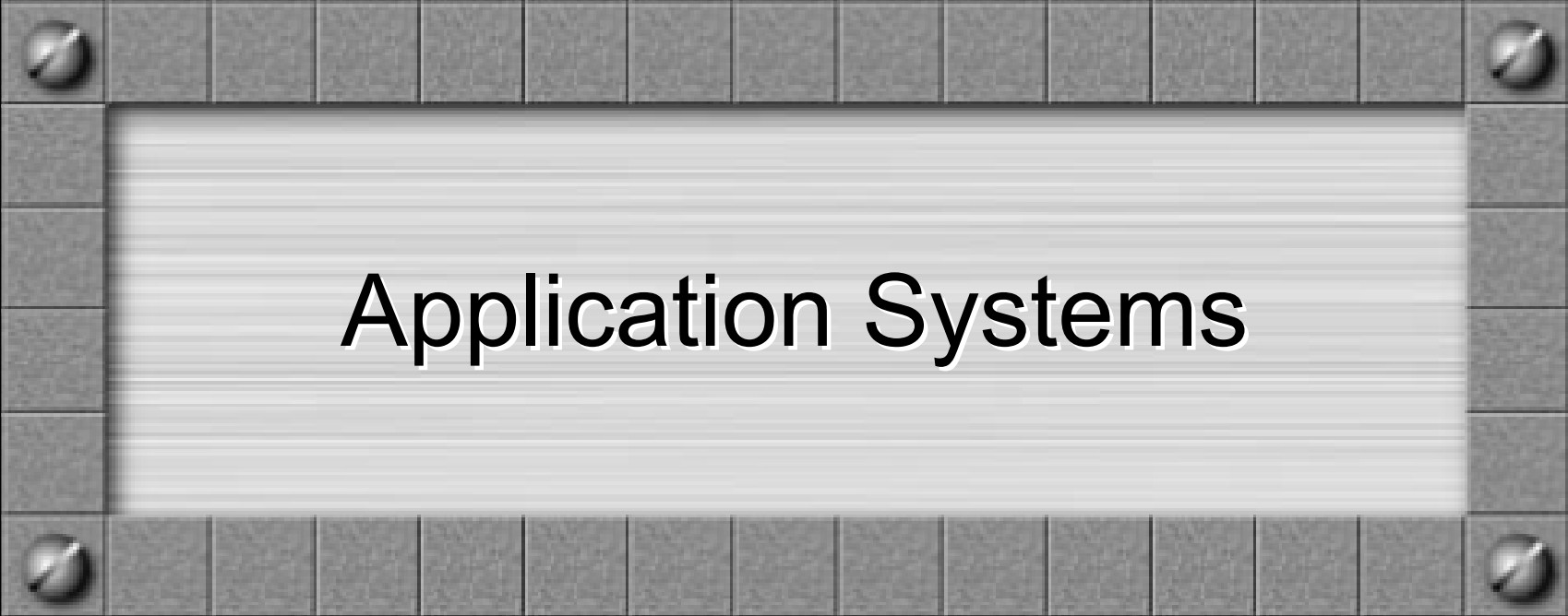
- ✓ Ensure that the plan's priorities support
 - ✦ Objectives of the organisation,
 - ✦ Meet regulatory requirements
 - ✦ Conform to contractual requirements.
- ✓ Verify that the plan ensures the survival of the organisation.
- ✓ Check for evidence that the priorities have been reviewed and accepted by management.
- ✓ Ensure that all critical applications have been identified.

BCP Audit: Strategies

- ✓ Verify that the strategies adopted by the company are in line with the priorities.
- ✓ Check for the implementation of the various components of the plan.
- ✓ Check whether the resources allocated for the plan are adequate.
- ✓ Review the list of suppliers to be contacted.
- ✓ Determine whether the plan clearly indicates how movement to the recovery site is to be effected.
- ✓ Examine the adequacy of telecommunications backup.
- ✓ Evaluate the methods and frequency of data backups
- ✓ Determine the adequacy of offsite data storage.
- ✓ Evaluate the security of the offsite facility.
- ✓ Perform an inventory review at the offsite facility.

BCP Audit: Responsibilities and Tasks

- ✓ Ensure that the responsibilities and tasks assigned to various personnel are in accordance with the priorities and strategies.
- ✓ Evaluate the ability of IS personnel and other staff to respond effectively in a disaster.
- ✓ Ensure that the staff has participated in the development of emergency procedure.
- ✓ Test check contact information (of vendors, employees) to ensure that they are current.
- ✓ Ensure there is no excessive dependence on any one person.



Application Systems

Application Systems

- ✓ Point of Sale Systems (POS)
- ✓ Electronic Fund Transfer (EFT)
- ✓ Automatic Teller Machine (ATM)
- ✓ Imaging Systems
- ✓ EDI
- ✓ Electronic Commerce

Point of Sale Systems (POS)

- ✓ Capture data at the time and place a sale transaction occurs
- ✓ Online
 - ✦ Directly connected to the back end.
- ✓ Batch
 - ✦ POS device holds the sale information for a certain predefined time period after which the data is transferred to the main computer.

Electronic Fund Transfer (EFT)

- ✓ credit transfers between banks where funds flow directly from the payer's bank to the payee's bank
- ✓ High-risk areas
- ✓ Security and access control are extremely important
- ✓ Individual access to the system is granted by a two-factor authentication system.

Automatic Teller Machine (ATM)

- ✓ Specialized form of point of sale terminal designed for the unattended use by a customer of a financial institution
- ✓ Internal control guidelines for ATMs
 - ✦ Bank personnel should not be able to retrieve or display customers' PIN numbers.
 - ✦ PIN should be entered only by the cardholder and only in an environment that deters casual entry observation.
 - ✦ PIN should not be transmitted in unencrypted form.
 - ✦ Cards should be mailed to customers in envelopes with a return address that does not identify the bank.
 - ✦ Cards and PINs should be mailed separately.

Imaging System

- ✓ Examples and benefits
 - ✦ Better service and productivity
 - ✦ Security
 - ✦ Disaster Preparedness

Fundamentals of EDI

✓ Definition

- ✦ EDI is defined as the transmission, in a standard syntax, of unambiguous information of business or strategic significance between computers of independent organisations.
 - ✦ EDI communicates information pertinent for business transactions between the computer systems of companies, government organizations, small businesses, and banks.
- ✓ Key benefit of EDI is reduction of transaction costs

EDI Architecture

- ✓ EDI Semantic Layer
- ✓ EDI Standard Layer
- ✓ EDI Transport Layer
- ✓ Physical Layer

EDI Semantic Layer	Application Level Services	
EDI Standard Layer	EDIFACT ANSI X.12	
EDI Transport Layer	E-Mail PPP WWW	X.435 MIME FTP, Telnet HTTP
EDI Physical Layer	Dial-up, Leased	

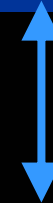
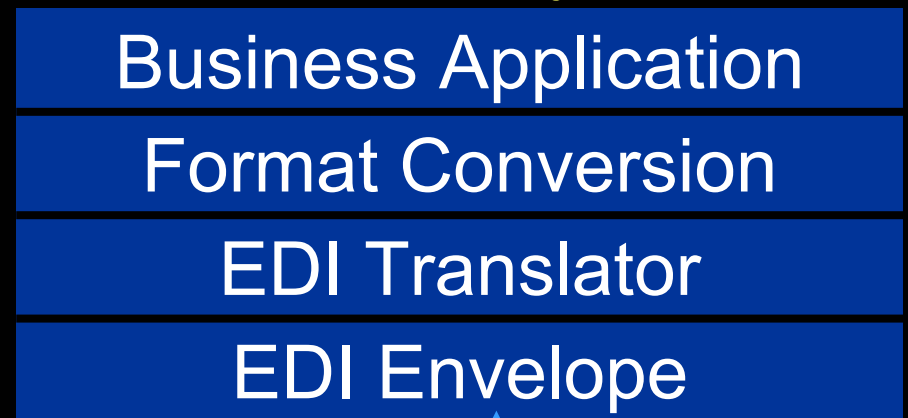
EDI Software Implementation

- ✓ Business Application
- ✓ Internal Format Conversion
- ✓ EDI Translator
- ✓ EDI Envelope for Document Messaging

Company A



Company B



VAN, Internet

EDI Standards

✓ ANSI ASC X.12

- ✦ American National Standards Institute-Accredited Standards Committee

✓ UN/EDIFACT

- ✦ United Nations/ Electronic Data Interchange for Administration Commerce and Trade

✓ UN/XML

- ✦ United Nations/ eXtensible Mark-up Language

EDI Risks, Controls and Audit

- ✓ Risks of EDI
- ✓ EDI Controls
- ✓ Auditing EDI

Risks of EDI

- ✓ Improper transaction authorization
- ✓ Manipulated/deleted between the application and EDI translator.
- ✓ Loss or duplication of EDI document.
- ✓ Loss of confidentiality.

EDI Controls

- ✓ Direct or dedicated lines to reduce the risk of interception
- ✓ Encryption of messages.
- ✓ Use of sequence number.
- ✓ Message authentication codes (MACs) and digital signatures.
- ✓ Special acknowledgement transactions or functional acknowledgments.

EDI Controls

- ✓ Controls to ensure that all inbound EDI transactions are
 - ✦ Accurately received (communication phase),
 - ✦ Translated (translation phase) and
 - ✦ Passed to an application (application interface phase) and
 - ✦ All inbound EDI transactions are processed only once.
- ✓ Controls to ensure that only properly authorized outbound transactions are sent.

Auditing EDI

- ✓ Verify that the software performs an authorization check against trading partner master file to ensure that the trading partner number and authorized transaction types are authorized.
- ✓ Ensure that fields undergo reasonableness edit checks to ensure that the data is accurate.
- ✓ Ensure that all inbound transactions are logged.
- ✓ Ensure the continuity of message serial numbers.
- ✓ Review the functioning of EDI system to ensure that functional acknowledgements are properly sent.

Electronic Commerce Models

- ✓ B2B
- ✓ B2C
- ✓ C2C
- ✓ C2B
- ✓ C2G/G2C

Interfaces to Legacy and ERP Systems

- ✓ Electronic Commerce (EC) systems typically interface with most of the other systems in an organisation.
- ✓ Enterprise Resource Planning (ERP) is a complete enterprise wide business solution that attempts to integrate all departments and functions in a company into a single computer system.
- ✓ An ERP system consists of software modules for business areas such as: marketing and sales, field service, product design and development, production and inventory control, procurement, distribution, industrial facilities management, process design and development, manufacturing, quality, human resources, finance and accounting, and information services.

Third Party Assurance Services

- ✓ Four types of concerns
 - ✦ Security of Data
 - ✦ Privacy of Data
 - ✦ Business Policies
 - ✦ Transaction Processing Integrity
- ✓ WebTrust Seal



Thank You

Mathew A Thomas
mat@vsnl.com