Controlling & Auditing
Information System

Magister SI UNIKOM

IT Controls

Basuki Rahmad, Dr, CISA, CISM

Agenda

- Introduction
- IT and the audit process
- IT controls model
- Planning an IT controls review
- Documenting IT systems
- Organisation and management controls
- IT operations
- Physical and environmental controls
- Logical access controls
- Change management
- Third party service providers
- End user computing
- Intro to application controls
- Application security
- Input, process, output controls
- Masterfile/standing data controls
- Case studies and revision
- Module review

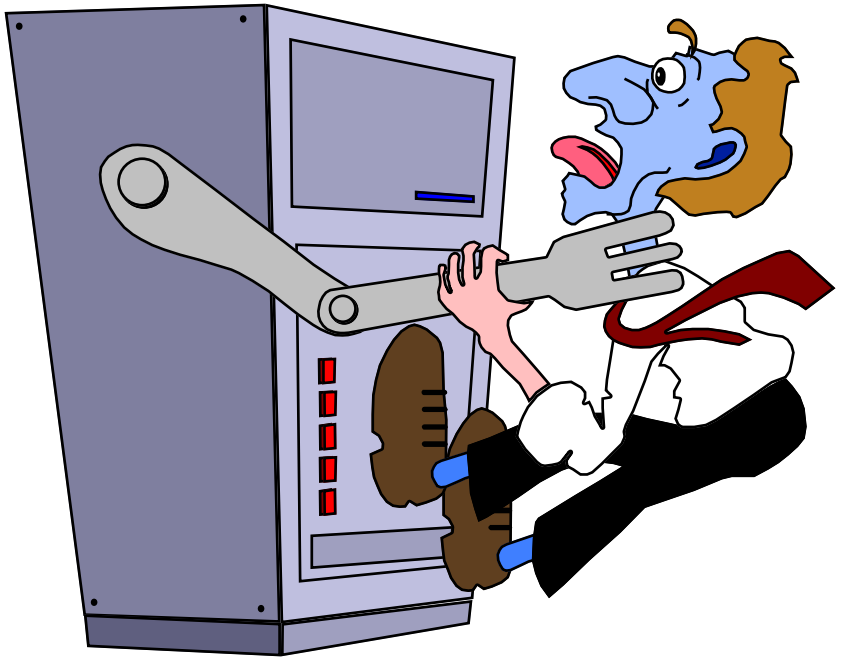
IT and The Audit Process

Changes in internal controls

- Computerisation has changed the type and nature of internal controls.
- Categories :
  - Personnel controls
  - Segregation of duties
  - Authorisation and accountability controls
  - Record keeping
  - Access to assets and records
  - Management supervision and review

New causes and sources of error

- System generated transactions
- Systematic error



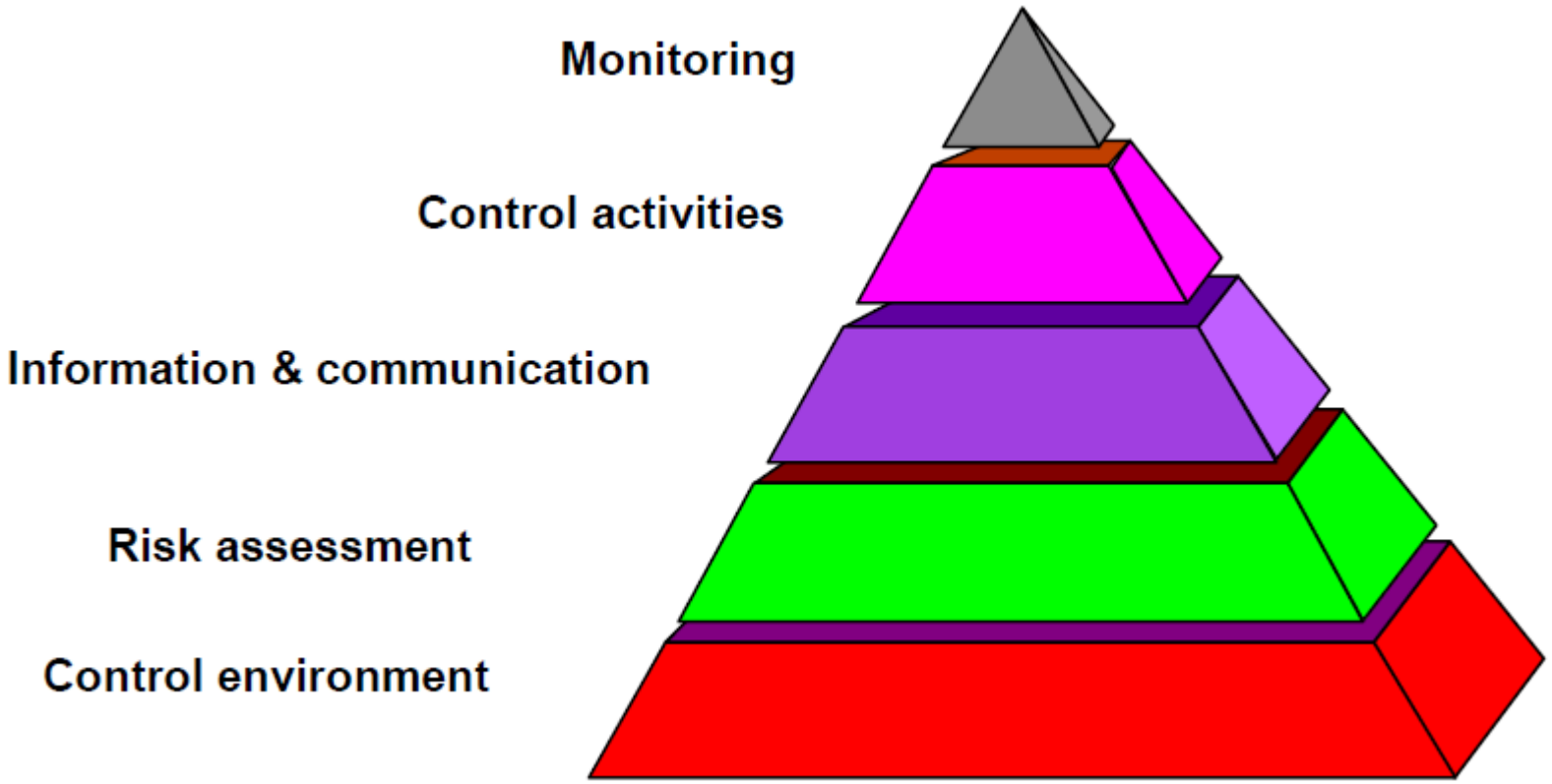
IT Controls Model

Controls

- Controls are aimed at different systems, e.g
  - Accounting controls
  - Operational controls
  - Administrative controls

- Control categories
  - Preventative controls
  - Detective controls
  - Corrective controls

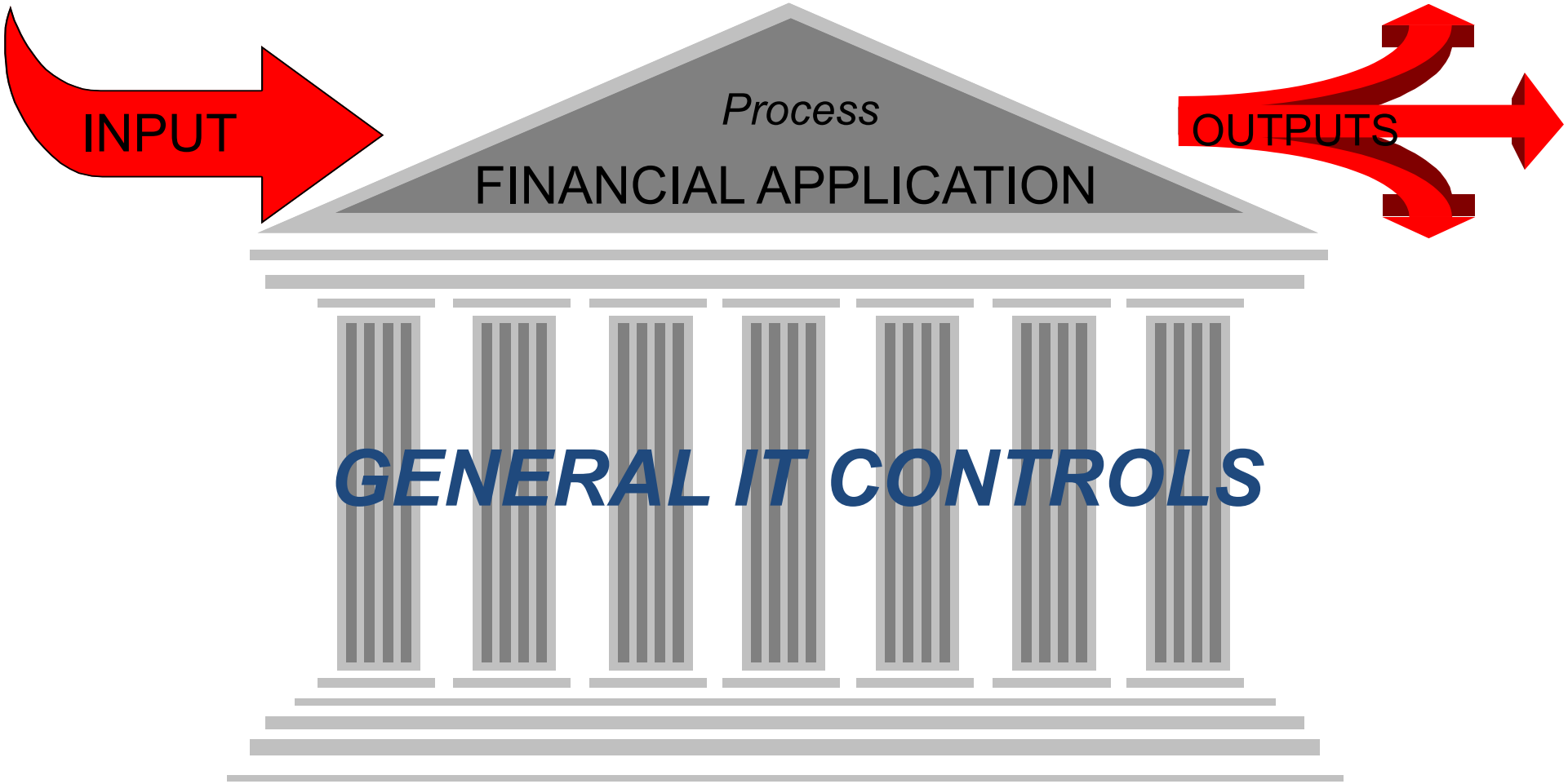
Elements of internal control environment



Limitations of internal controls

- Provide reasonable, not absolute assurance
- Obsolescence due to changes in a system
- Depend on involvement of people
- Management's power to overrule or bypass controls

General & Application Controls



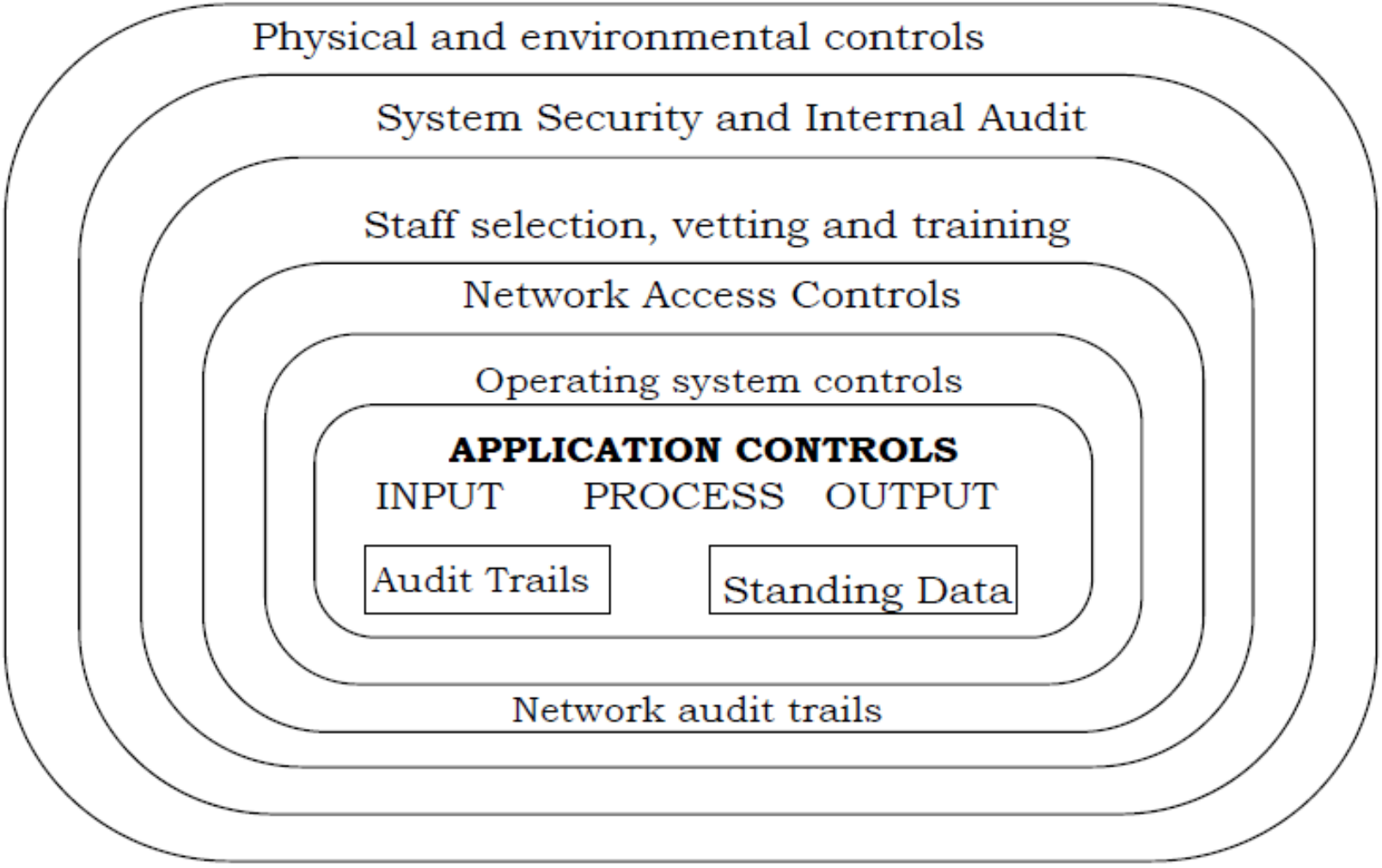
General IT Controls

- Organisation and management controls
- Segregation of duties
- Physical and environmental controls
- Logical access controls
- System development and program change controls
- IT operations controls
- Business continuity planning
- End user computing controls

Application Controls

- Particular to an application, and have a direct impact on processing of individual transactions
- Main areas of control:
  - Input controls
  - Processing controls
  - Output controls
  - Standing data, masterfile controls
- General controls provide the applications with the resources needed to operate

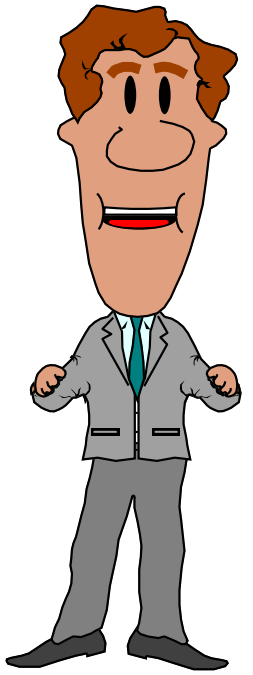
IT Control Framework



Planning IT Controls Review

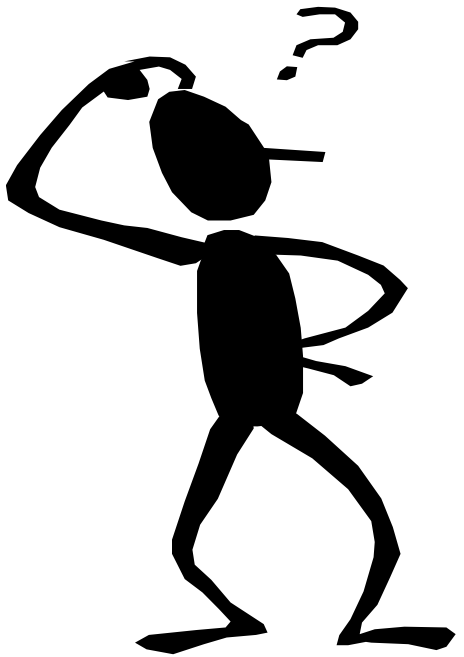
Session Objectives

- To introduce the planning stage of an IT controls review
- To identify the key steps involved when planning an IT controls audit
- To describe the circumstances under which an IT specialist would be required to carry out an IT controls review.



Why carry out a controls review ?

- Client request
- Sponsor’s request
- Legal, regulatory requirements



Knowledge of the client

- The organisation and operations of the client.
- The financial reporting requirements
- The legal and regulatory environment
- Who are the stakeholders and what interest do they express in the client's business
- The client's accounting process, including the use of computers

Knowledge of the client's IT and internal control environment

Questions to resolve

- Are there any problems the auditor should know about?
- Does the client intend to make any changes?
- What systems does the client have ?
- Who will I need to talk to/interview to get the information I need ?

Sources of information

- Last year’s auditor
- Last year’s working papers
- Observation
- Interviewing IT personnel.
- Reviewing internal audit reports
- Key client documents

The need for computer specialists

- Where particular risks have been identified
- Where the client demands a specialist
- Where systems development is prevalent
- Where changes are expected, new systems planned.



IT audit services

- During audit planning
  - Documenting the client's IT systems
  - Identifying and evaluating audit risks
  - Provision of advice on auditing specific accounting packages
  - Identifying and evaluating key controls
  - Assessing opportunities for using computer assisted audit techniques (CAATs)
- During the audit (testing/evidence gathering)
  - Test controls
  - Use of CAATs tools/techniques
  - Report system failures, computer problems to the financial auditor
- After the audit
  - Contribution to client reports or management letters

Nature extent and timing of audit procedures

Which systems to review ?

- Contribution of each system to the financial statements
- The terms of the engagement
- The size and complexity of the systems
- Higher risk transactions/ balances
- Known weaknesses in internal control or a history of errors

Timing of audit involvement

- Financial audit IT controls reviews
- IT controls reviews

Documenting IT Systems

Objectives

- To enable IT auditors to decide which systems need to be documented
- To introduce systems documentation techniques

Commonly encountered financial systems/ subsystems/ modules

- Sales
- Purchases
- Stock
- Cash management
- Asset management
- Payroll
- Grant management
- Job costing

Understanding the system

- Level of detail required
  - Controls review
  - Financial audit : controls reliant or substantive

- Enables the financial auditor to:
  - understand the flow of transactions (completeness)
  - choose an effective audit approach
  - channel resources to the higher risk areas
  - comply with auditing standards and guidelines

Sources of information

- Discussion
- Client documentation
- Internal audit reports
- Accounting records, system reports, input /output forms

Systems documentation methods

- Flowcharts
- Narratives
- Questionnaires

Flowcharts

- Flowcharts:
  - Graphical representation of the flow of transactions
  - Usually produced from a top down perspective.
  - They usually integrate the computerised and manual elements of a system in one document
- Advantages:
  - Brevity
  - Usually easier to understand and review
  - Can show flow of transactions through the processing and recording cycle
  - Inconsistencies and omissions and relationships are more apparent·
  - Show spans of control
  - Updating simpler

Flowcharts

- Disadvantages:
  - Staff training / experience required
  - The auditor may be tempted to include too much detail into the flowcharts,
  - They can be limited in scope and may not identify managerial or organisational controls.
  - Symbols and conventions are not uniform
  - They can be time consuming to prepare.
- Principles:
  - Standardisation, Simple and concise
  - Left to right flows
  - Vertical bands to represent sections
  - Explain significant documents
  - Minimum narrative

Narrative

- Descriptions:
  - System objectives and targets
  - Processes and procedures
  - Links and interfaces with other systems
  - Controls
  - What happens when exceptional conditions occur
  - Ad hoc controls
- Advantages:
  - They provide details of the procedures and controls in operation.
  - They can provide a precise coherent description of the system
  - Quick to produce
  - Easier to produce
  - They are useful when describing unique or special transactions

Narrative

- Disadvantage:
  - Cumbersome
  - They can be difficult to interpret
  - Interrelationships may not be clearly shown

Questionnaires

- Descriptions:
  - Based on a series of questions on the client's systems and procedures
  - ICQs aimed at determining if control objectives are satisfied
  - Normally require a yes/no answer from the auditor NOT the client
  - Aimed at the auditor
  - Can be preprinted (proformas)
- Limitations:
  - What do you believe are the limitations of using questionnaires to document and assess the internal controls within a client's financial systems?

Organization and Management Controls

Objectives

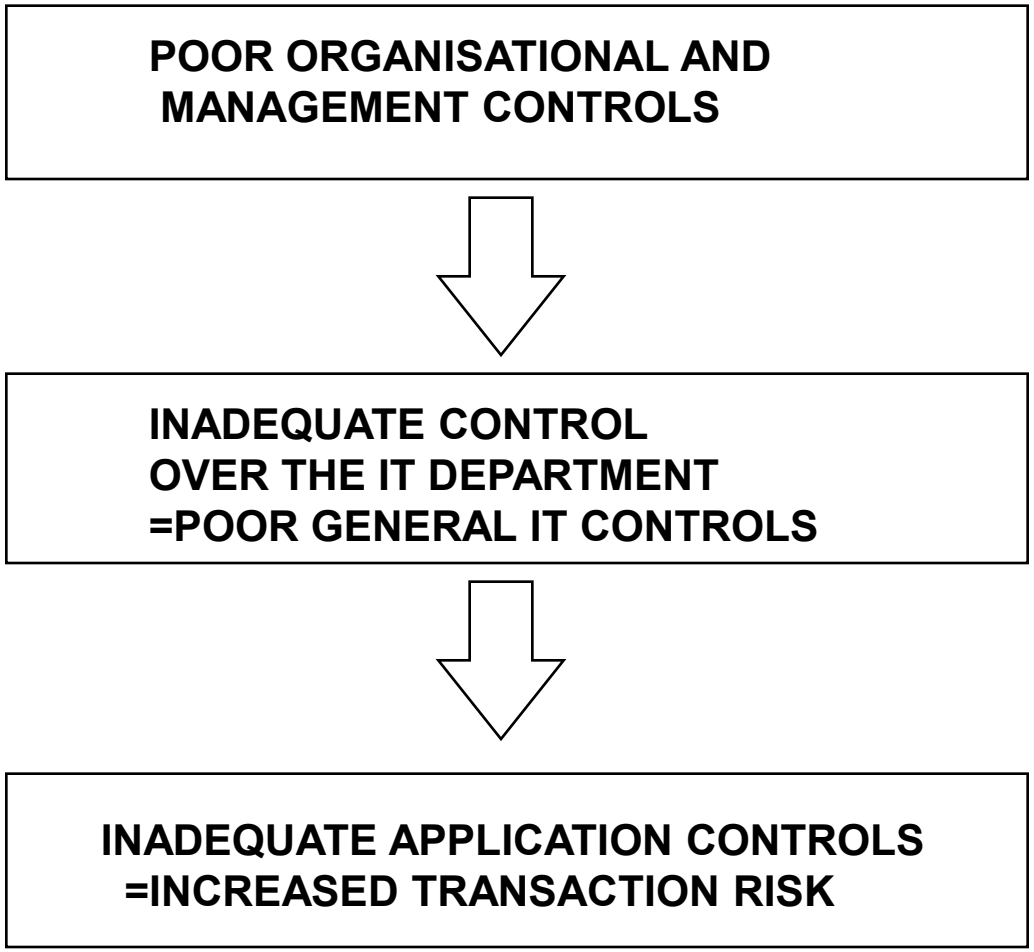
- To consider the importance of IT organizational and high level management controls to an IT environment.
- To review the types of management control likely to be encountered by an IT auditor
- To review the role of separation of duties within an IT department
- To enable the IT auditor to identify weaknesses in a client's organization and put forward constructive recommendations

Components of IT organization and management

- Risks
- IT organizational structure
- IT strategy
- IT Personnel
- Documentation
- Segregation of duties
- Third party supplier policies
- Internal audit
- IT security policies
- Legal issues

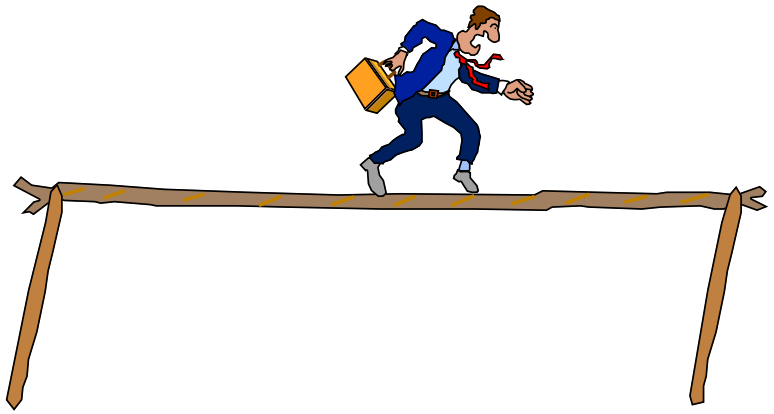


Flow of controls

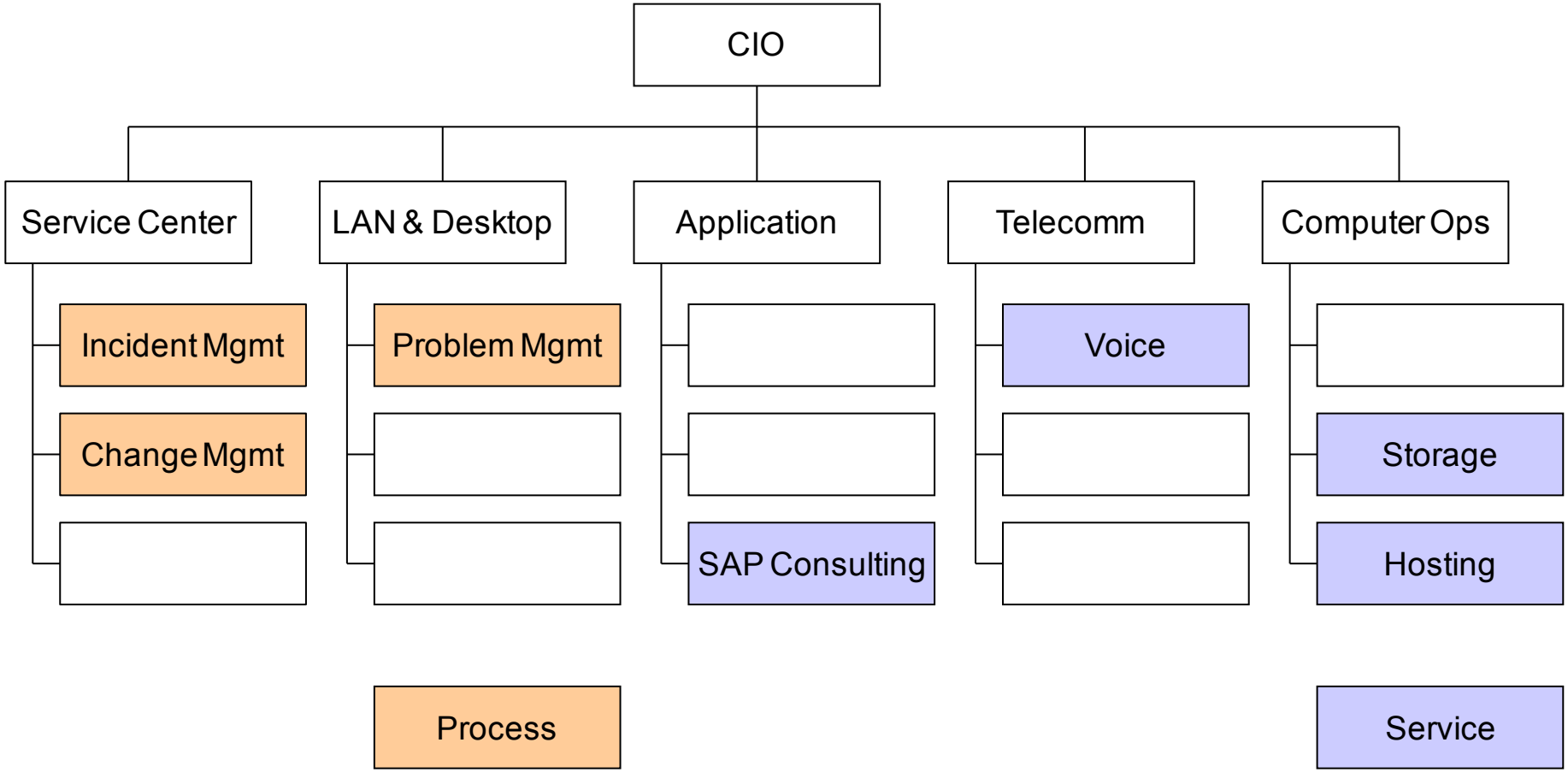


What are the risks?

- Why does the client need IT organization and management controls?
- What risks could arise from a poor controls in this area?
- What impact could a lack of adequate controls have on the external auditor?

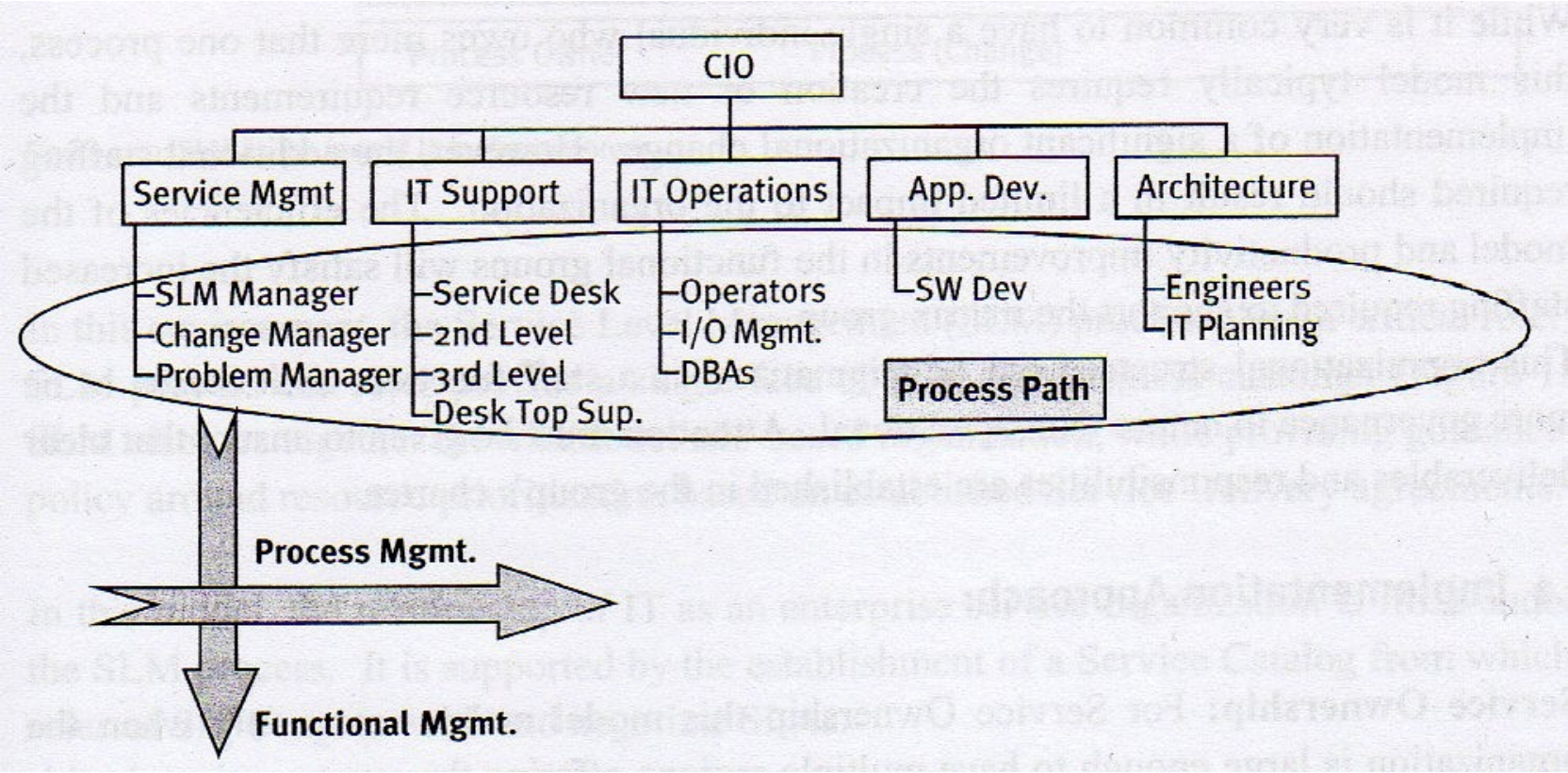


IT Organization Chart



Ownership Model 1: Placing ownership within existing structure

IT Organization Chart



Ownership Model 2: IT Service Delivery Function

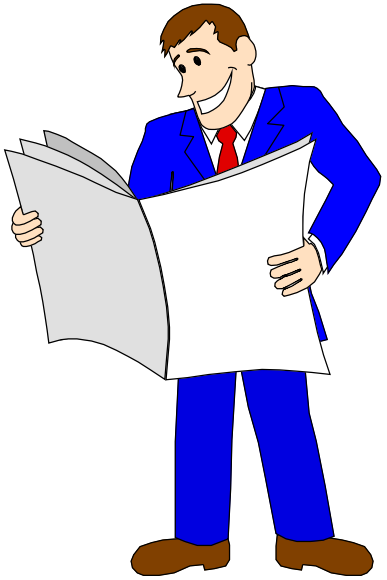
Senior management control and involvement

- Overall responsibility for IT
- The existence of an organizational structure
- Senior management's involvement in controlling the direction and management of IT services
  - Steering committees



IT strategy

- Follow business needs/ future strategy
- Forward looking
- Review and update
- Awareness
- Systems covered
- Approval



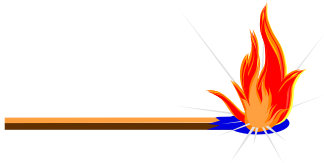
Audit issues

- Should the external financial auditor care if the client has no IT strategy ?
- If we care, what would we do about it ?

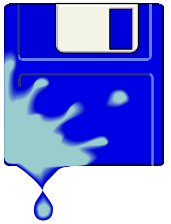
Causes of errors, loss, problems

1. Accidental/ unintentional people mistakes/ errors and omissions





2. Natural disasters
3. Fraud
4. Hardware / software failure



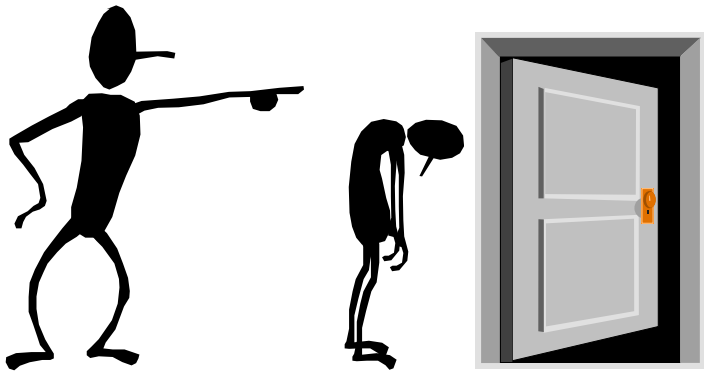
Personnel policies

- Organizational structure / charts
- Job descriptions
- Staff planning
- Training and staff development
- Staff assessments
- Special contracts
- Job rotation
- Vacation policies



Personnel policies

- Recruitment policies
  - Background checks
  - Confidentiality agreements
  - Codes of conduct
- Termination policies
  - Voluntary
  - Involuntary
  - Immediate termination
  - Security measures
  - Notification
  - Final pay
  - Leaving interviews
  - Return of property



System documentation policies

Risks associated with inadequate policies

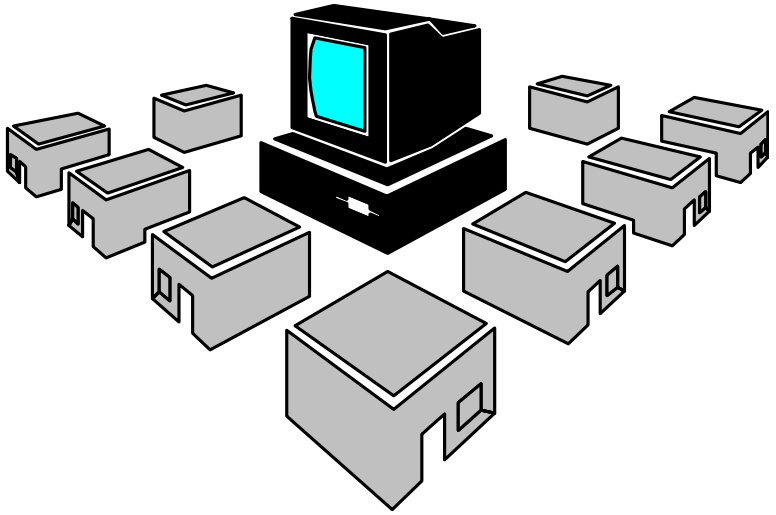
- Unauthorized working practices
- Increased errors, problems with the systems
- Systems maintainability problems

Documentation retention policies

- Evidence required to provide an opinion on the financial statements or provide an assessment of the controls environment.
- Evidence requirements dependent upon the audit approach.
  - Controls reliant
  - Substantive
- Consider other interested parties

Outsourcing policies

- Increasing trend
- Policy may influence future external audit involvement
- Ensure needs of external auditor are identified and known to client



Internal audit involvement

- Management sets policies
- Internal audit checks compliance with management's policies
- Questions to ask include:
  - Reporting freedom
  - Management / IA relationship
  - Scope of reviews / limitations
  - Resourcing
  - Quality

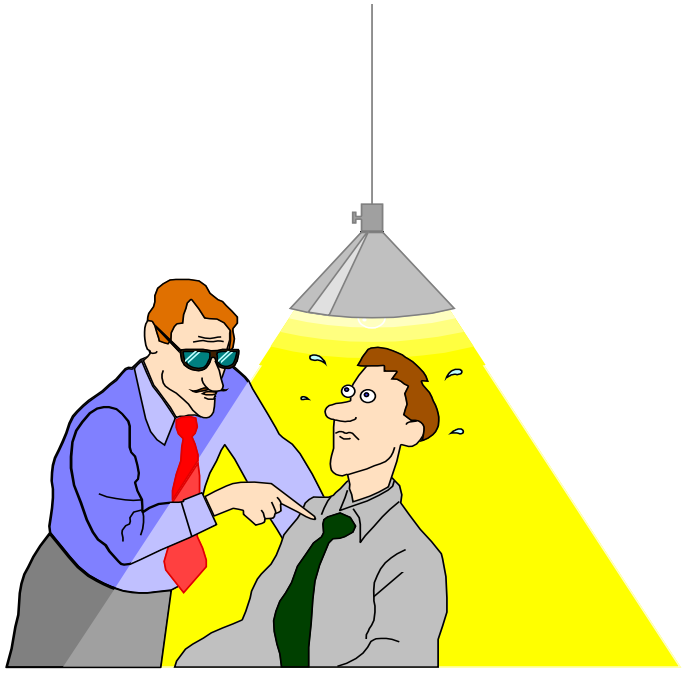
IT security policy

- Normally a concise narrative
- Senior management approved
- Availability
- Contents:
  - Definition of information security
  - Statement of management intention,
  - Specific security policies, principles, standards and compliance requirements
  - General and specific responsibilities
  - Security incident reporting



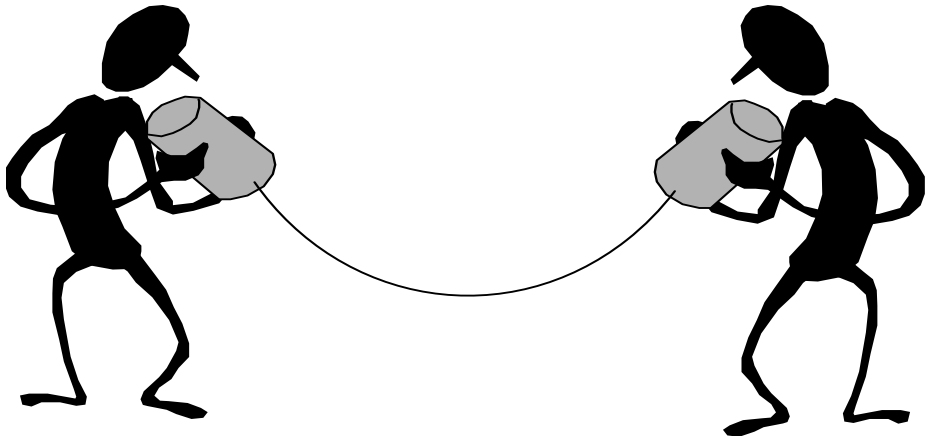
Legal and regulatory compliance

- Varies from country to country
- May include rules/ laws regulations for:
  - Data protection and privacy
  - Computer use/ misuse
  - Banking and finance regulations
  - Copyright laws / theft of software



Segregation of Duties

- Fundamental control concept
- Programmers and operators
- In a ideal environment all functions would be segregated
- Problems, limited scope in small clients
- Segregation between IT and users





Terimakasih

Thank You

Matur Nuwun

Hatur Nuhun