Information Security at KFUPM

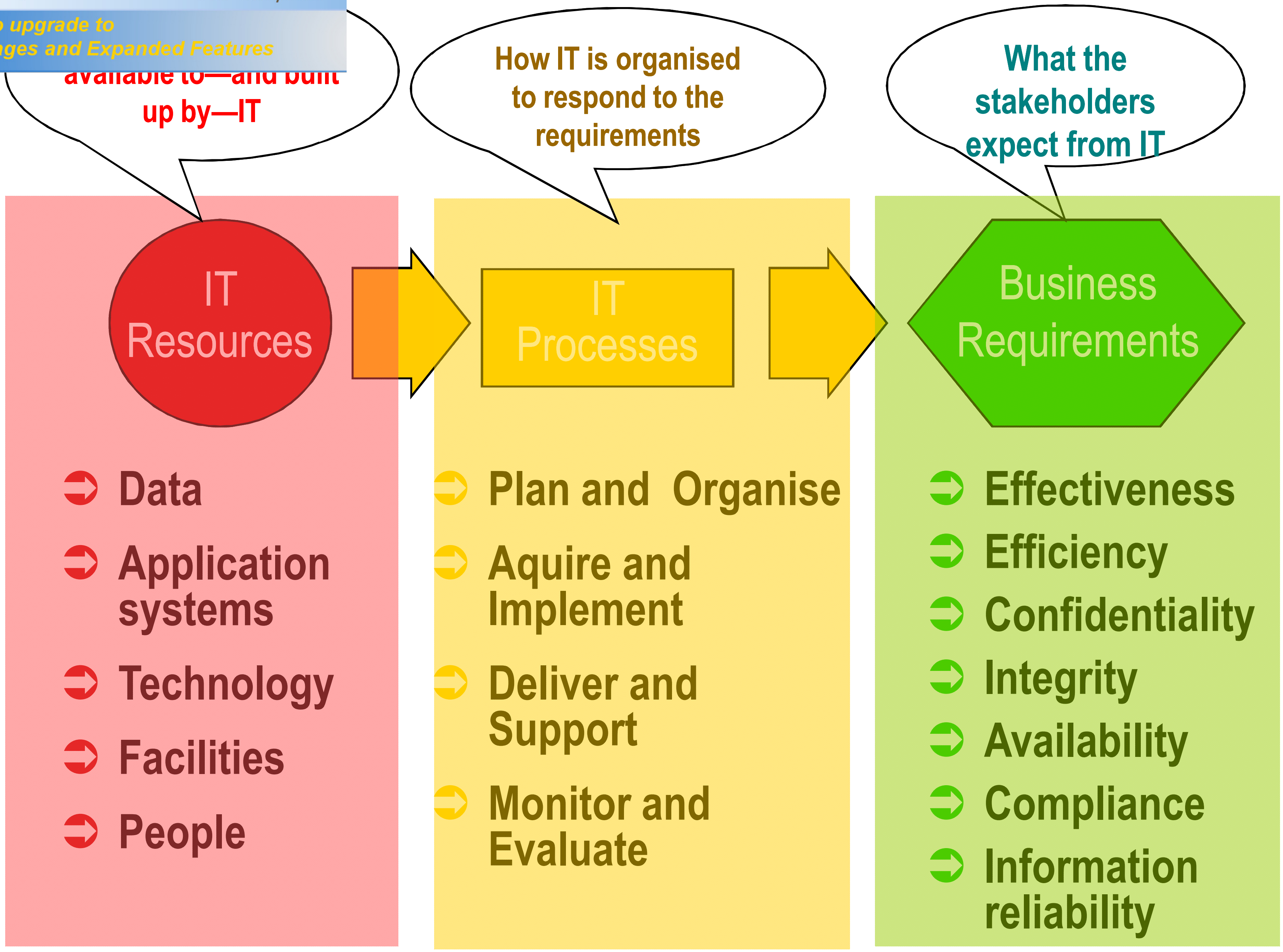
Mian Zainulabadin Khurrum

Certified Information Systems Security Professional (CISSP)
Certified Information Systems Auditor (CISA)

Manager Network Services

Why Information Security

- Should be looked at as a Business Enabler
- Essentially a risk mitigation process
- Management needs to accept that security is a process, not a project
- Security is an architecture unto itself, however it is also an infrastructure that spans the enterprise



available to—and built up by—IT

How IT is organised to respond to the requirements

What the stakeholders expect from IT

IT Resources

IT Processes

Business Requirements

- Data
- Application systems
- Technology
- Facilities
- People

- Plan and Organise
- Aquire and Implement
- Deliver and Support
- Monitor and Evaluate

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Information reliability

THE CIA triad

- Confidentiality
  - For e.g. Data Classification
- Integrity
  - For e.g. Auditing
- Availability
  - For e.g. Disaster Recovery

rk Security Architectures
Fortress Model

- Anyone outside the gate is suspect
- Anyone inside is trusted
- Static, undifferentiated
- Difficult to change
- Location-specific
- Reliant on strong walls and a secure gate

rk Security Architectures
Airport Model

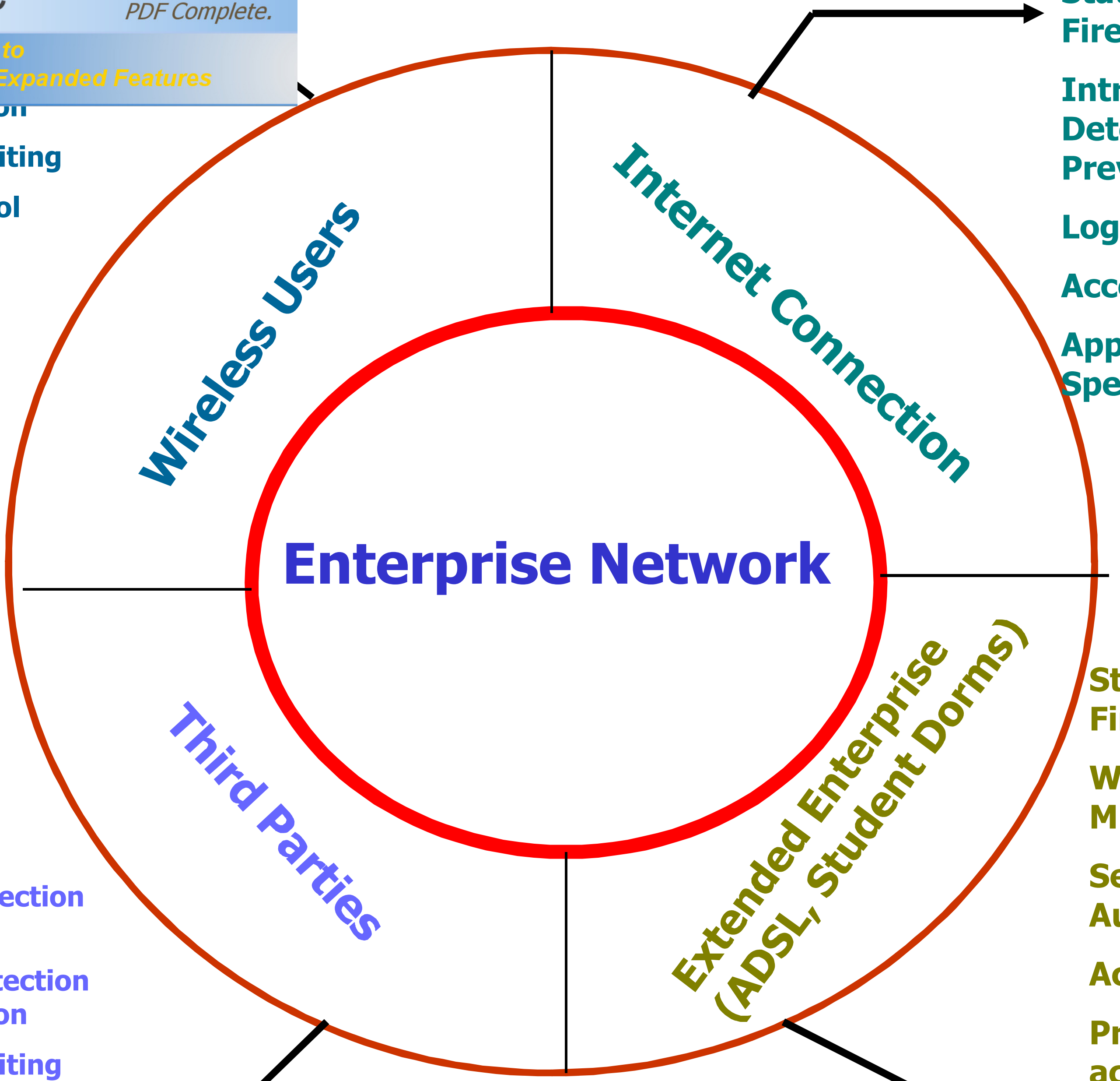
- Multiple security zones, based on roles
- Flexible and situational
- Multiple over-lapping technologies for identification, authentication and access control
- Series of fortresses within the master fortress

and Prevention

Logging, Auditing

Access Control

Encryption



Stateful Inspection Firewall

Intrusion Detection and Prevention

Logging, Auditing

Access Control

Application Specific Firewalls

Stateful Inspection Firewall

Intrusion Detection and Prevention

Logging, Auditing

Authentication and Authorization

Stateful Inspection Firewall

Worm Attack Mitigation

Selective Logging, Auditing

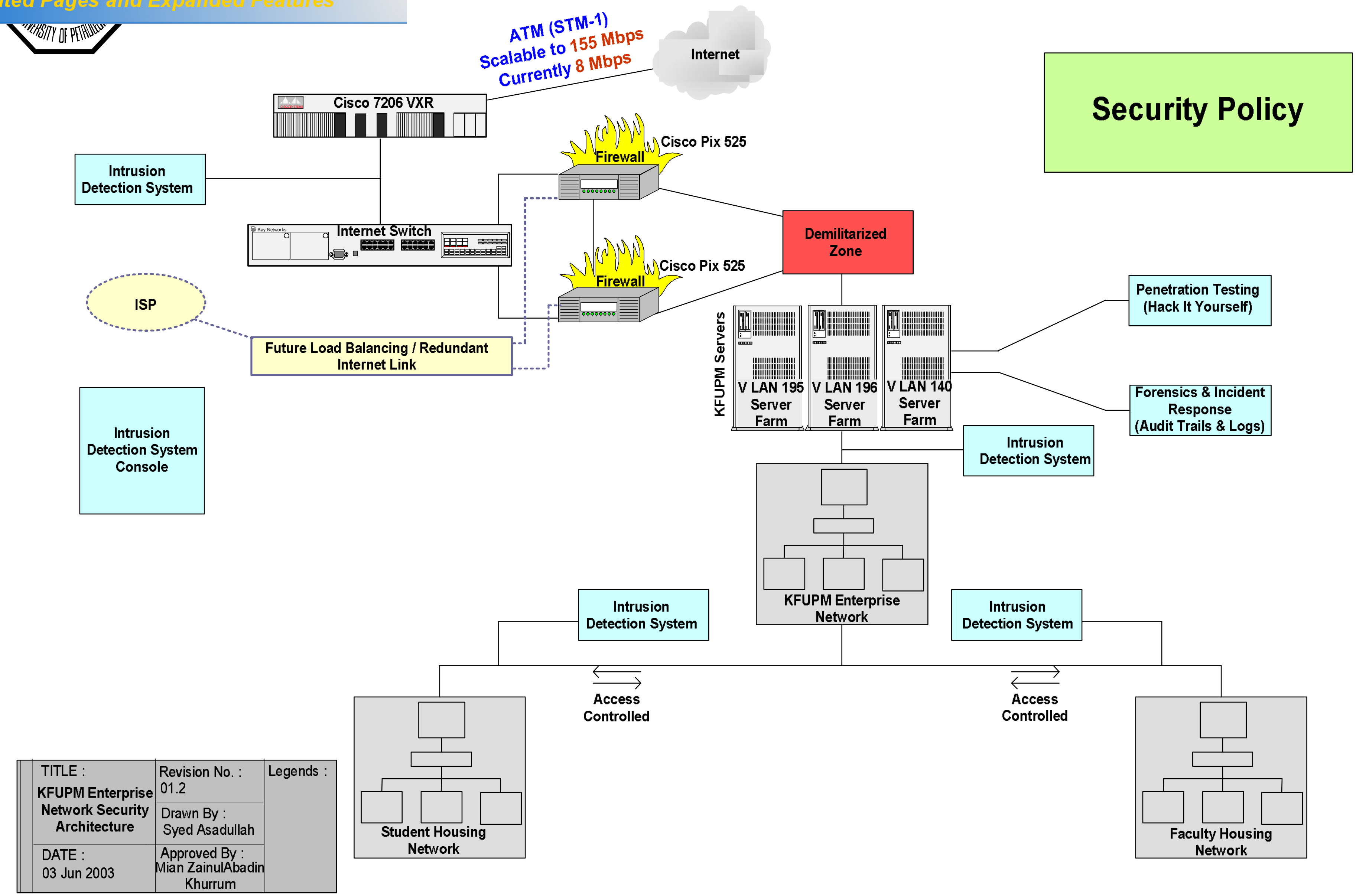
Access Control

Provide secure access to internal hosts

ork Security Architecture Point-to-Point dynamic trust

- No absolute trust for anyone
- Dynamic authentication and authorizations
- Suitable for E-Commerce and Virtual enterprises

Campus Network Security Architecture



Security Policy

TITLE : KFUPM Enterprise Network Security Architecture	Revision No. : 01.2	Legends :
	Drawn By : Syed Asadullah	
DATE : 03 Jun 2003	Approved By : Mian ZainulAbadin Khurrum	

nore to Information Security

- Security Policy
- Organizational Security
- Asset classification and control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- System Development and Maintenance
- Business Continuity Management
- Compliance

How to achieve a secure IT environment acting as a business enabler ?

Adopt a Control Framework Based on International Standards

nportant International Standards

- COBIT (Control Objectives for Information Technology)
- ISO-17799 (Information Security Standard)

s IT need a control framework?

- Increasing dependence on information and the systems that deliver this information
- Increasing vulnerabilities and a wide spectrum of threats, such as cyberthreats and information warfare
- Scale and cost of the current and future investments in information and information systems
- The need to comply with regulations. Not relevant for SA
- The potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs
- Recognition by many organisations of the potential benefits that technology can yield

Successful organisations understand and manage the risks associated with implementing new technologies.

s IT need a control framework?

To ensure that

- IT provides value
  - Cost, time and functionality are as expected
- IT does not provide surprises
  - Risks are mitigated
- IT pushes the envelope
  - New opportunities and innovations for process, product and services

management needs to get IT under control

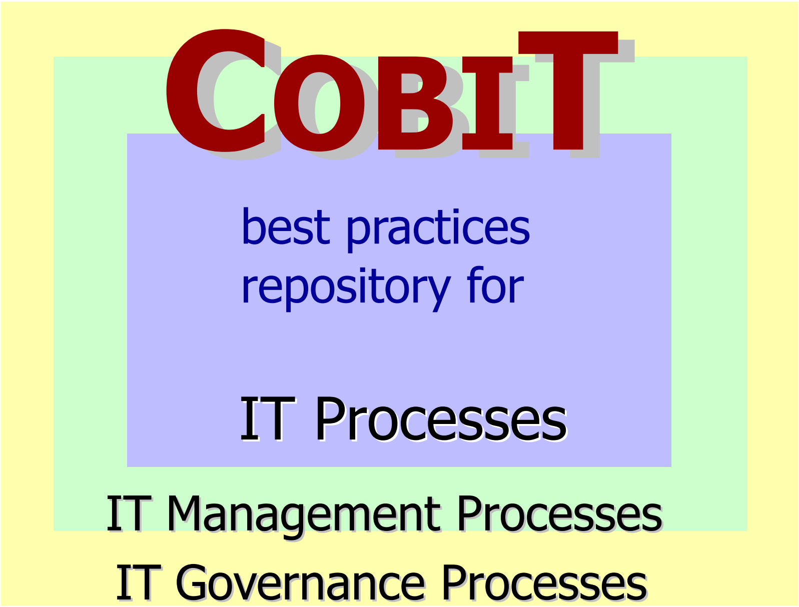
a control framework?

- Board and Executive
  - To ensure management follows and implements the strategic direction for IT
- Management
  - To make IT investment decisions
  - To balance risk and control investment
  - To benchmark existing and future IT environment
- Users
  - To obtain assurance on security and control of products and services they acquire internally or externally
- Auditors
  - To substantiate opinions to management on internal controls
  - To advise on what minimum controls are necessary

w is COBIT used?

COBIT as a response to the needs

- Incorporates major international standards
- Has become the de facto standard for overall control over IT
- Starts from business requirements
- Is process-oriented



what does it consist?

- ➢ Starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives
- ➢ Promotes process focus and process ownership
- ➢ Divides IT into 34 processes belonging to four domains and provides a high-level control objective for each
- ➢ Considers fiduciary, quality and security needs of enterprises, providing seven information criteria that can be used to generically define what the business requires from IT
- ➢ Is supported by a set of over 300 detailed control objectives

- ● Plan and Organise
- ● Acquire and Implement
- ● Deliver and Support
- ● Monitor and Evaluate

- ● Effectiveness
- ● Efficiency
- ● Availability
- ● Integrity
- ● Confidentiality
- ● Reliability
- ● Compliance

ISO I7799: 10 Areas

- **Security policy:**
  - Adopting a security process that outlines an organization's expectations for security, which can then demonstrate management's support and commitment to security.
- **Security organization:**
  - Having a management structure for security, including appointing security coordinators, delegating security management responsibilities and establishing a security incident response process.
- **Asset classification and control:**
  - Conducting a detailed assessment and inventory of an organization's information infrastructure and information assets to determine an appropriate level of security.
- **Personnel security:**
  - Making security a key component of the human resources and business operations. This includes writing security expectations in job responsibilities (IT admins and end users), screening new personnel for criminal histories, using confidentiality agreements when dealing with sensitive information and having a reporting process for security incidents.
- **Physical and environmental security:**
  - Establishing a policy that protects the IT infrastructure, physical plant and employees. This includes controlling building access, having backup power supplies, performing routine equipment maintenance and securing off-site equipment.

ISO I7799: 10 Areas

- **Communications and operations management:**
  - Preventing security incidents by implementing preventive measures, such as using antivirus protection, maintaining and monitoring logs, securing remote connections and having incident response procedures.
- **Access control:**
  - Protecting against internal abuses and external intrusions by controlling access to network and application resources through such measures as password management, authentication and event logging.
- **Systems development and maintenance:**
  - Ensuring that security is an integral part of any network deployment or expansion, and that existing systems are properly maintained.
- **Business continuity management:**
  - Planning for disasters--natural and man-made--and recovering from them.
- **Compliance:**
  - No clear for Saudi Arabia. However Auditing Framework should be established to comply with adopted standards.

How to approach security

- Establishing Security Requirements
  - Three main sources
    - Risk Assessment
      - Cdentified, evaluated and estimated
    - Legal, Statutory, Regulatory
      - Contractual requirements the organization must fill. Perhaps not relevant for Saudi Arabia. Do we have a contract with students ?
    - Principle and Objectives
      - Requirements to support operations

Assessing Risks

- Risk Assessment
  - Considered on a systematic basis
    - Business impact to CIA
    - Likelihood of impact – threat vs controls
  - Guides and determines actions and priorities
    - Process of selecting controls is iterative per business unit and system
    - Reviews based on
      - Changing business requirements
      - New threats and vulnerabilities
      - Confirmation that current controls are effective
  - Assessments performed at a high level and then more specifically for detailed risk.

Selecting Controls

- Should be selected based on a cost benefit analysis.
- Reputation should also be a factor in that decision.

InfoSec Guiding Principles

- InfoSec Best Practices
  - Information security policy document
  - Allocation of information security responsibilities
  - Information security education and training
  - Reporting security incidents
  - Business continuity management

Information Security Policy

- To provide management direction and support for information security.
- A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization’s approach to managing information security.
- Policy owner should periodically review the policy; on effectiveness, efficiency and controls.

Information Security Policy

- Essential Requirements:
  - Definition of InfoSec, objectives and scope.
  - Management statement of support.
  - Definition of responsibilities of management in InfoSec.
  - Brief explanation of policies, principles standards and compliance.
  - References to documents that support the policy with details for specific systems.

Information Security Management System (ISMS)

- Manage and maintain secure information system environment
    - A framework to facilitate a relationship between processes and products.
    - Implementation and maintenance or process and procedures; and must address the following,
        - ID InfoSec needs
        - Strategy to meet those needs
        - Measurement of results
        - Improving strategies over time
    - Approach must be Hollistic
        - Human
        - Technology
        - Process

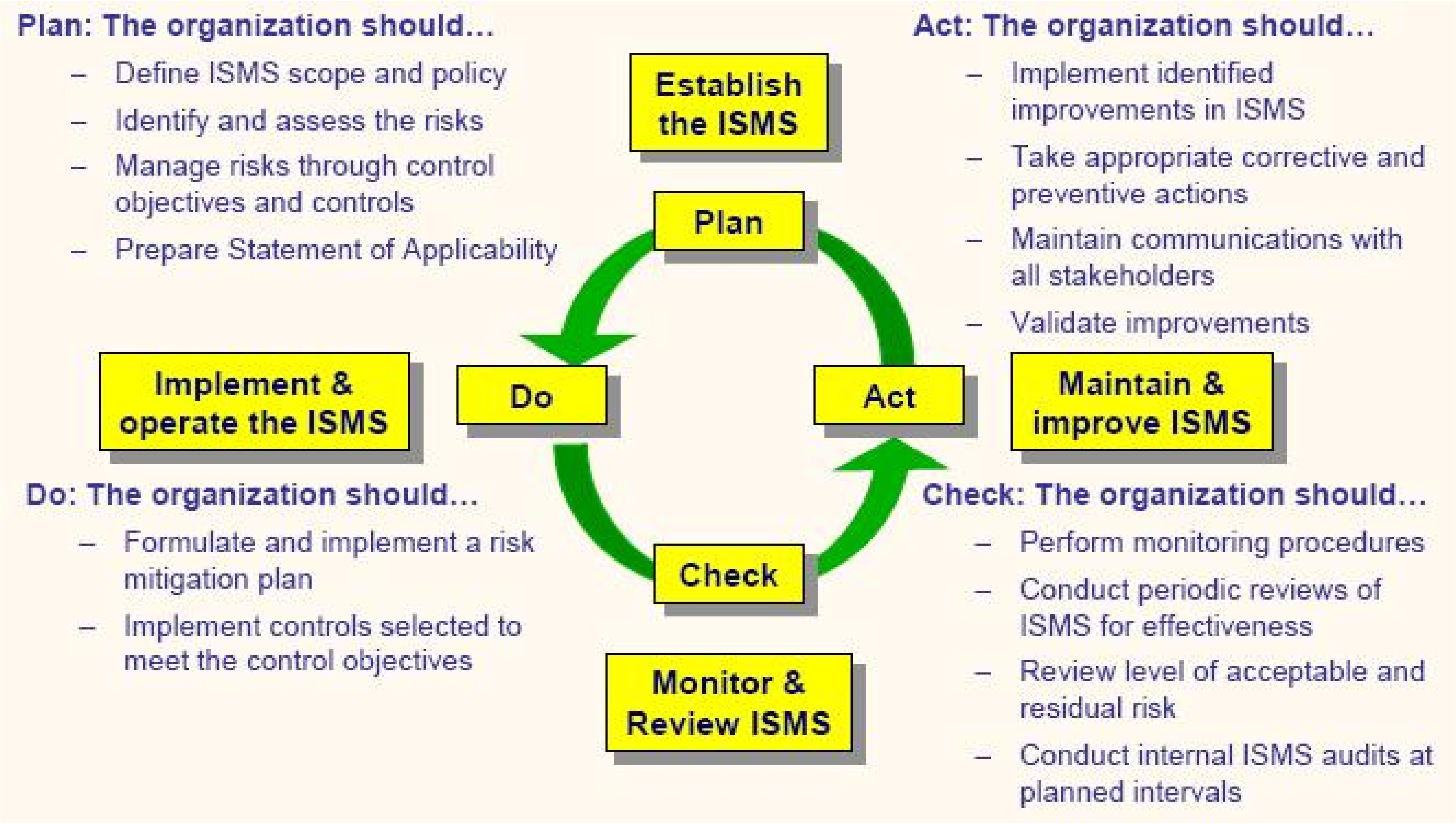
ISMS

- Process ISMS – security policy forms the basis of the process
  - Two phase approach
    - Planning
    - Implementation – the controls or guidelines as provided by ISO17799.
      - Assess whether the guidelines apply
      - Third party audit
  - First step: pick a process
    - Implement process ex. New employee screening
    - Then check to see if all new employees are screened
  - Second step: check for compliance
    - Plan-Do-Check-Act
    - Iterative process that requires feedback
    - Must be tailored to fit

ISO17799 A Blue Print

1. KFUPM decides to implement
2. Senior Management must visually commit to adopting the standard
3. Decide InfoSec Policy
4. InfoSec policy once adopted must be furnished to all trained employees
5. Senior Mngmt then decides which business units will be offered up for certification
6. The orgs scope for this project produces an SMS Scope Doc
7. The Risk Assessment (RA) is carried out for the Scope Doc(ID asset , threat , vuln.).= RA doc
8. KFUPM decides risk approach and determines acceptable degree of risk
9. KFUPM must decide to how to manage the identified risk so that residual deg. of risk is within acceptable limits.
10. Once action, accountability and ownership are established, it is documented
11. Controls to required to reduce risk to acceptable levels are identified.
12. Controls selected from ISO17799 and documented
13. Selected controls must be traceable to the risk they address. This is documented in the Statement of Acceptibality (SoA)

Achieving ISO Compliance



Plan: The organization should…

- Define ISMS scope and policy
- Identify and assess the risks
- Manage risks through control objectives and controls
- Prepare Statement of Applicability

Act: The organization should…

- Implement identified improvements in ISMS
- Take appropriate corrective and preventive actions
- Maintain communications with all stakeholders
- Validate improvements

Do: The organization should…

- Formulate and implement a risk mitigation plan
- Implement controls selected to meet the control objectives

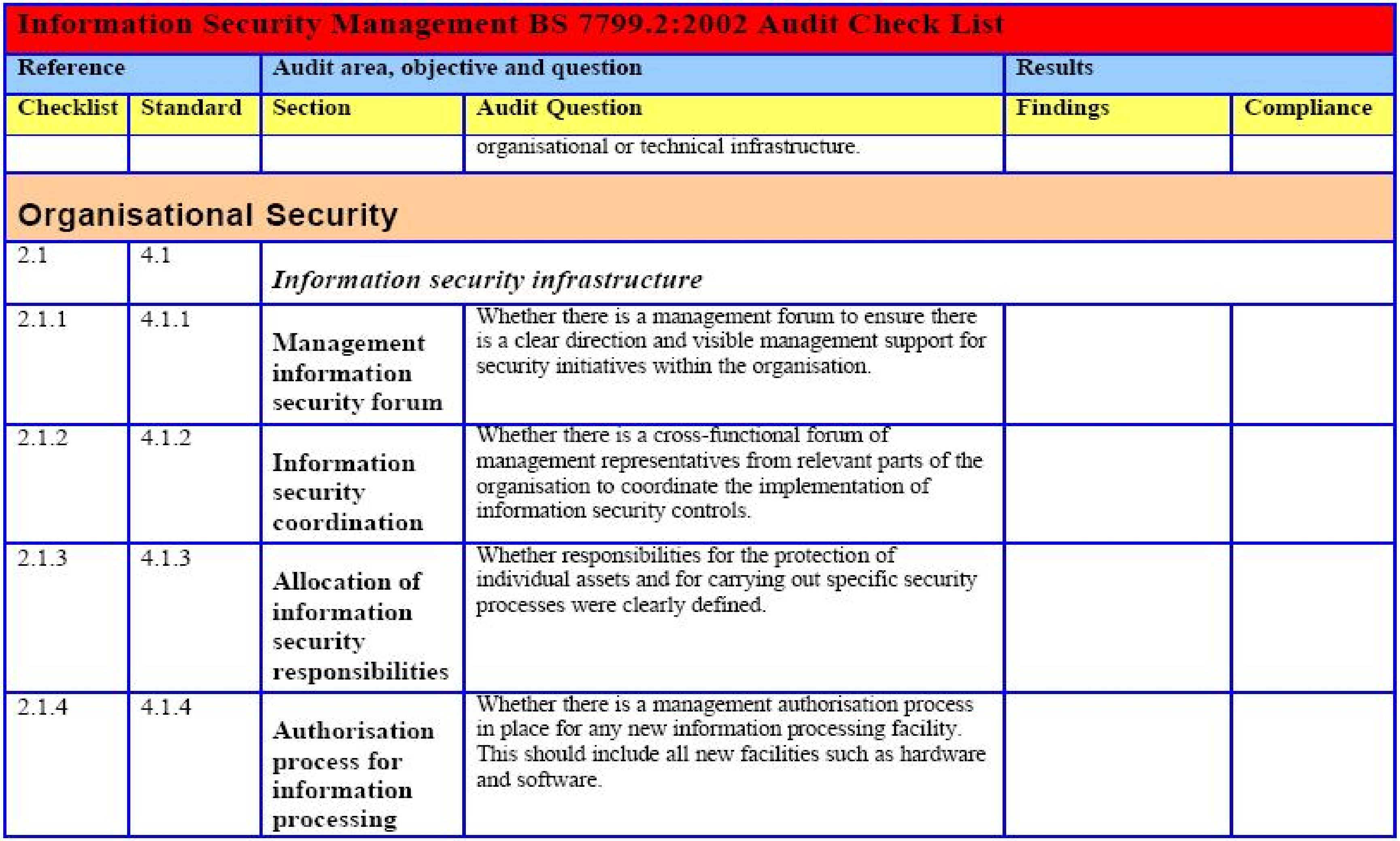
Check: The organization should…

- Perform monitoring procedures
- Conduct periodic reviews of ISMS for effectiveness
- Review level of acceptable and residual risk
- Conduct internal ISMS audits at planned intervals

Sans Auditing Template

- 10 Areas of Audit
  1. Security Policy
  2. Organizational Security
  3. Asset Classification and Control
  4. Personnel Security
  5. Physical and Environmental Security
  6. Communications and Operations Management
  7. Access Control
  8. System Development and Maintenance
  9. Business Continuity Planning
  10. Compliance
- **36 Control Objectives**
- **127 Controls**

Sans Auditing Template



Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
			organisational or technical infrastructure.		
Organisational Security					
2.1	4.1	*Information security infrastructure*			
2.1.1	4.1.1	Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.		
2.1.2	4.1.2	Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information security controls.		
2.1.3	4.1.3	Allocation of information security responsibilities	Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.		
2.1.4	4.1.4	Authorisation process for information processing	Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.		

Critical Success Factors

- Security policy, objectives and activities that reflect business objectives
- An approach to implementing security that is consistent with the organizational culture*
- Visible support and commitment from management*
- A good understanding of the security requirements, risk assessment and risk management
- Effective marketing of security to all managers and employees
- Distribution of guidance on information security policy and standards to all employees and contractors
- Providing appropriate training and education*
- A comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

ts have not been mentioned deliberately

- Firewall will make us secure
- PKI will make us secure
- IDS will make us secure
- DRP plan will make us secure
- ERP is a magic, will change KFUPM

Questions