
Deloitte.
IT GCC Audit
Back To The Basics

Introduction

- IT Audit Overview
- Control Framework
  - -COSO
  - -Cobit
  - -ISO17799
- Areas of General Computer Controls
  - -General Area of Risk
  - -Controls Objectives

IT Audit Overview
IT Auditor Perception

"We've all seen them before, those blue suits carrying shiny, leather briefcases: Auditors. They march into our shops, asking question after question, touching and probing everything connected to CAT 5. They check for everything from industry best practices to security standards to government regulations. This result is usually a thick report that grades your security program as pass or fail."

Source: "Surviving an Audit", George Wrenn. Information Security Magazine, April 2004.

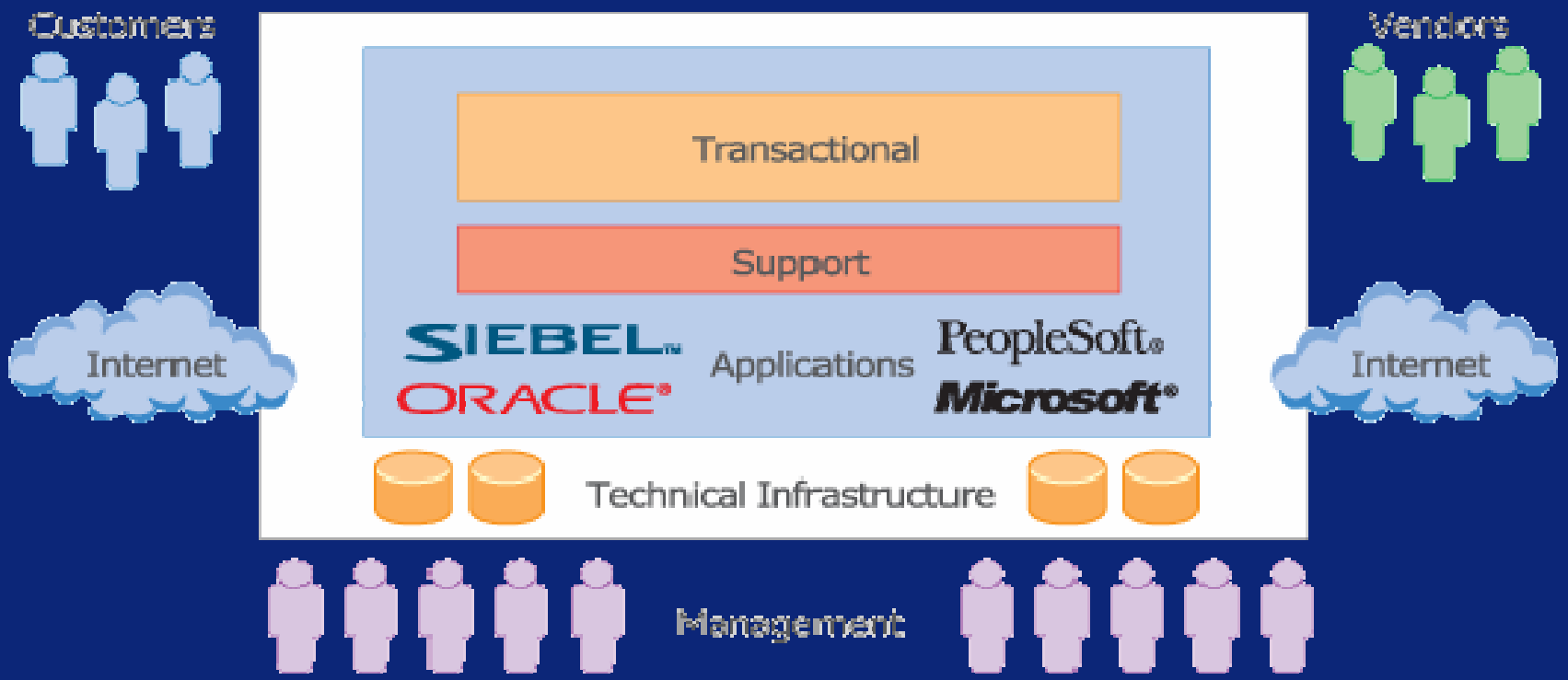
As IT Auditors, how would you like to be perceived?

IT Audit Overview
IT Auditor Reality

"But, auditors -- whether they're internal or third parties – are a security professional's friends. They are a second set of eyes looking at your policies, infrastructure and practices and verifying the areas in which you're doing well, and those that need work. Most importantly, they tell you how well you're complying with standards and regulations, such as ISO17799 and Sarbanes-Oxley."

Source: "Surviving an Audit", George Wrenn. Information Security Magazine, April 2004.

IT Audit Overview
The IT Environment



As technology has advanced, the legacy IT environment has evolved into the modern IT environment, which consists of many different physical machines all connected together in a network.

IT Audit Overview
The IT Environment

- Application Systems
  - Transactional
    - Financial, CRM, supply chain
  - Support
    - Email, calendar, MS Office
- Infrastructure
  - Network
  - Databases
  - Operating systems
  - Management

Where in the IT environment do you think the biggest IT risks lie?

IT Audit Overview
Accounting Systems

- Generally record and account for the financial impact of transactions processed
- Often integrated with other functional systems (e.g., ERP systems)
- Key risks
  - Loss of financial data
  - Fraud
  - Theft
  - Loss of ability to report

IT Audit Overview
HR Systems

- Maintain employee information
- Process payroll and benefits
- Key risks
  - Payroll losses
  - Loss of sensitive information

IT Audit Overview
CRM Systems

- Maintain customer information
- Often drive the sales process
- Key risks
  - Poor customer service
  - Loss of sales opportunities
  - Lost sales orders

IT Audit Overview
Manufacturing and Production Systems

- Maintain inventory
- Drive production processes
- Key risks
  - Loss of business continuity
  - Lost revenue
  - Inaccurate inventory balances
  - Sub-optimal operations

IT Audit Overview
Support Applications

- Support systems generally facilitate business activities, but do not typically process transactions directly
- Key risks
  - Business disruption
  - Theft of sensitive company information (email)

IT Audit Overview
Security Systems

- Control access to IT resources
  - Physical
    - Doors, etc.
  - Logical
    - Network
    - Single sign-on
- Key risks
  - Unauthorized access to information
  - Loss, theft or destruction of critical information

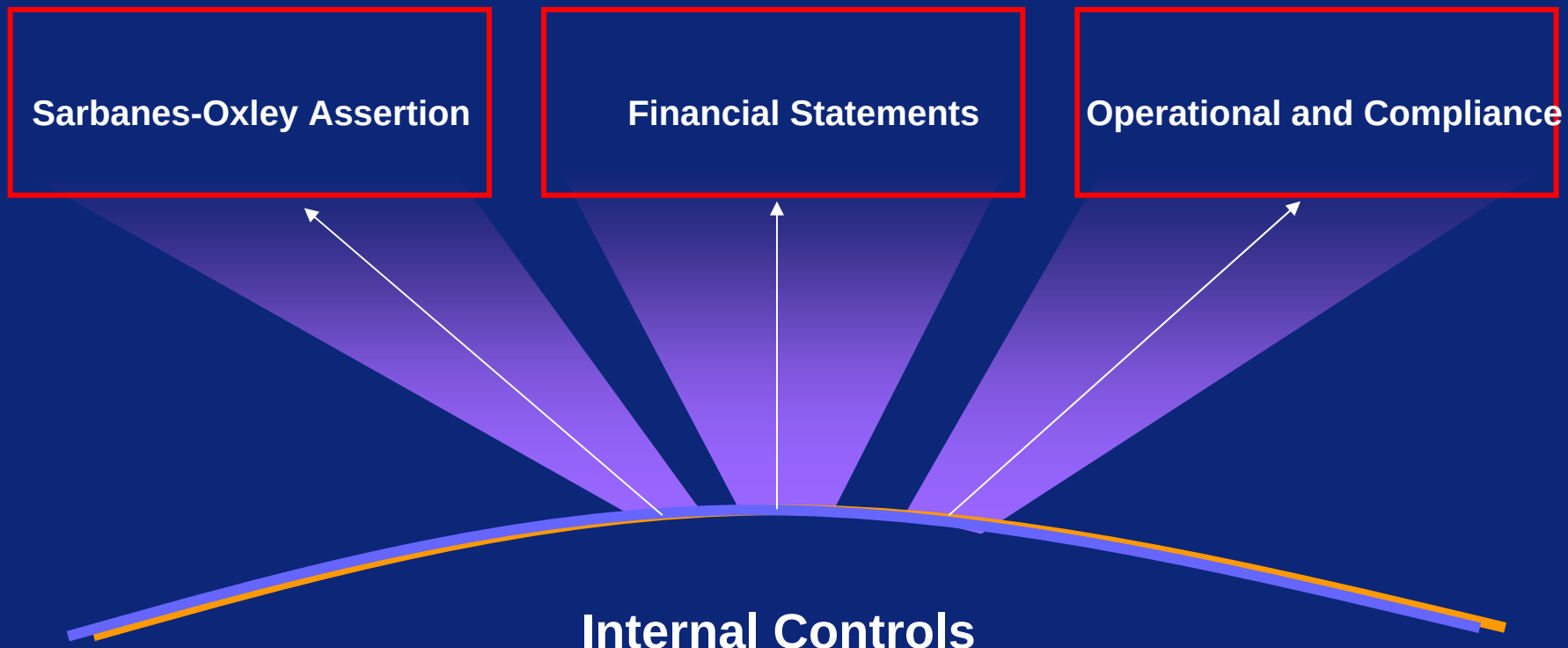
IT Audit Overview
Infrastructure

- Infrastructure supports the business applications
- All business transactions processed pass through infrastructure elements
- Key risks
  - Unauthorized access to critical data
  - Loss of transactions
  - Fraudulent transactions
  - Loss or destruction of data
  - Loss of business continuity

IT Audit Overview
IT Audit Function

- Help the organization manage IT risk
- Identification of IT controls
- Testing of IT controls
- Recommendations for enhancing IT control environment

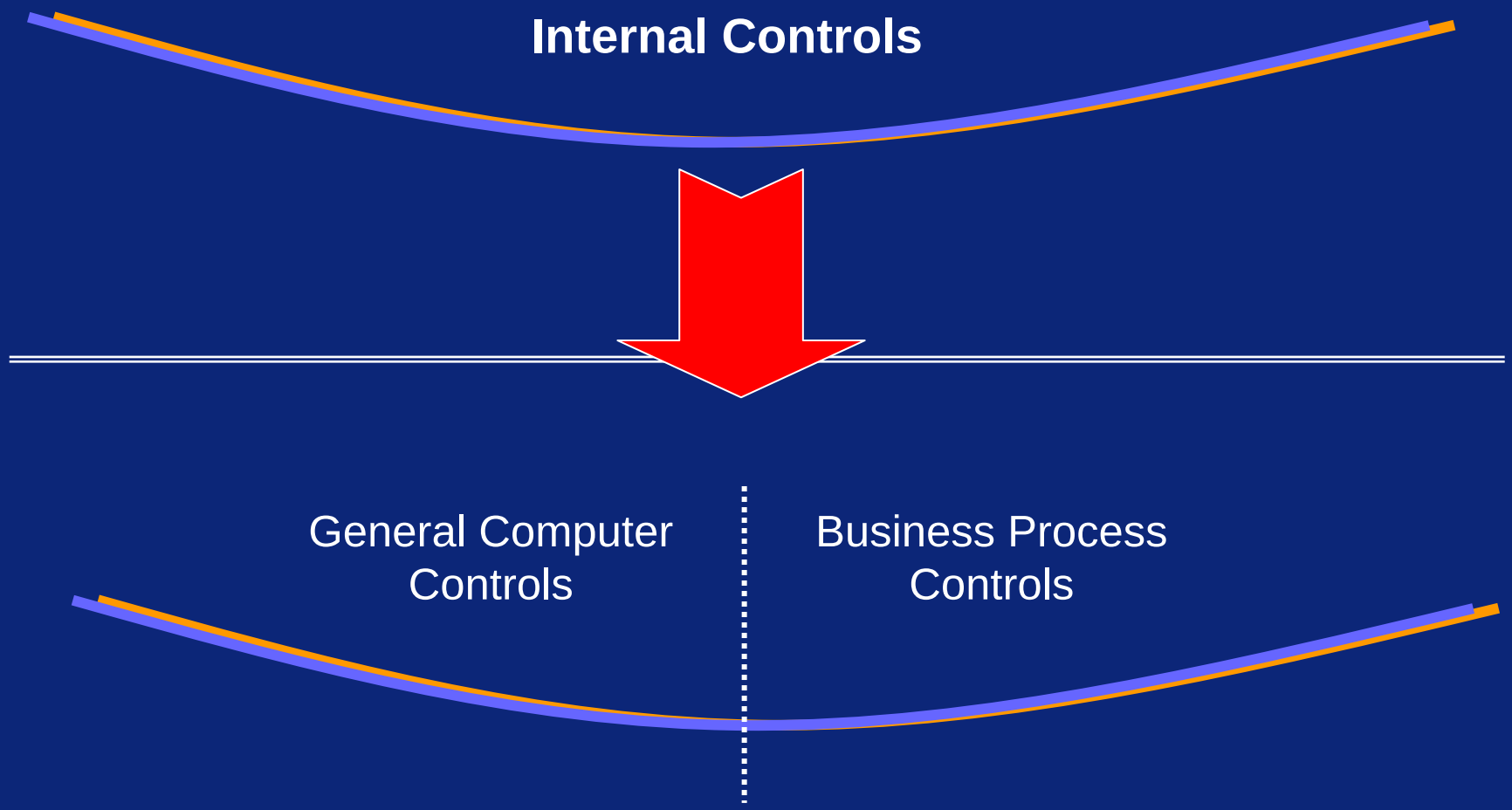
IT Audit Overview
Internal Controls Overview



IT Audit Overview
Internal Controls Definition

Policies and procedures that pertain to an entity's ability to initiate, record, process, and report financial data consistently with the assertions embodied in either annual financial statements or interim financial statement.

IT Audit Overview
Types of Internal Controls



IT Audit Overview
Types of Controls

IT controls can be further separated into two types of IT controls: business process controls and general computer controls.

Business Process Controls

General Computer Controls

General Computer Controls

- Controls inherent in IT infrastructure components
- Pervasive controls – not generally linked to any specific risk or business process
- Examples:
  - A firewall
  - Requiring a password to access the network

Business Process Controls

- Controls inherent in business processes
- Typically mitigate specific risks
- Generally aligned with specific business transactions
- Manual or based on systems
- Focus here on systems-based controls
- Examples:
  - Security access restrictions on who can post to the G/L in the financial application
  - Generation and review of a report listing errors in interfaced transactions

Control Framework
Why Select a Framework?

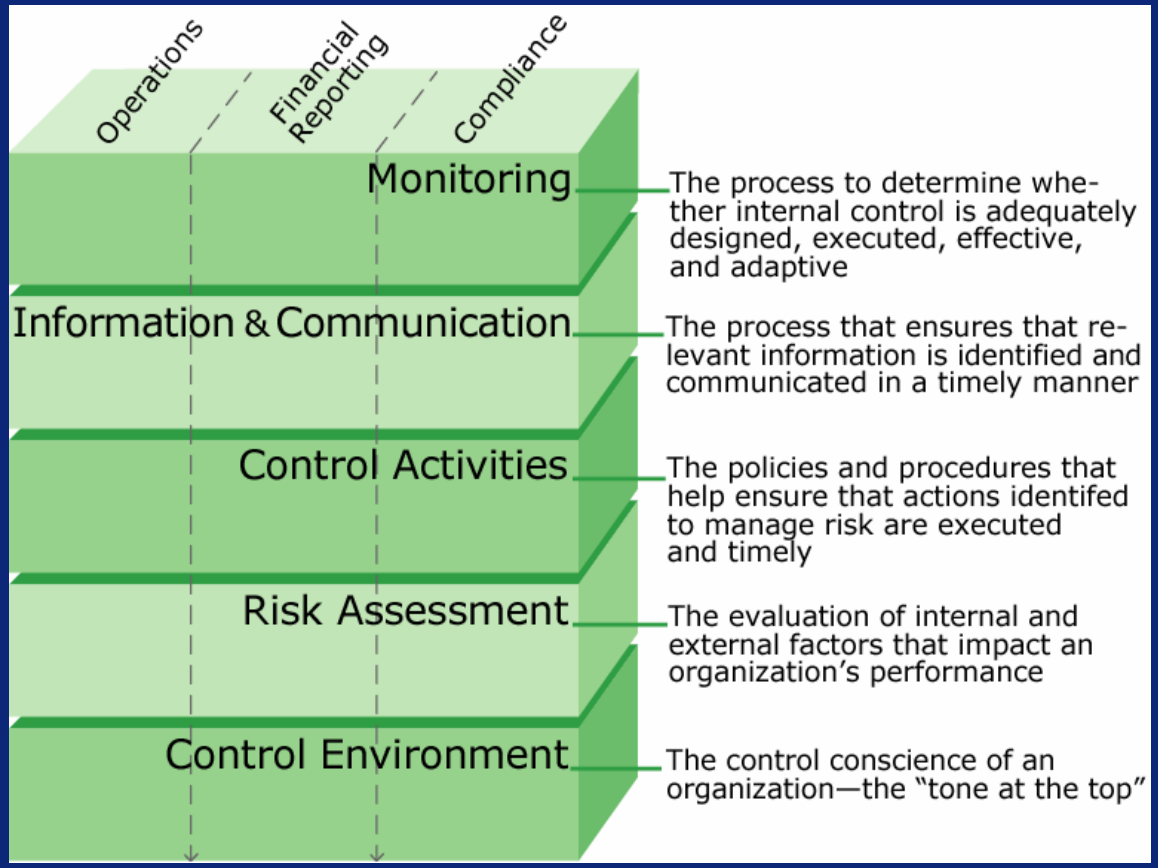
- Companies need a way of organizing their approach to IT
- Clear criteria for auditing are needed
- Section 404 of the Sarbanes-Oxley Act of 2002 requires management to annually:
  - State their responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting
  - Conduct an assessment of the effectiveness of the Company's internal controls over financial reporting as of year end
  - Include in their annual report a report by management asserting the existence and effectiveness of those internal controls
- Regardless of the method selected, a common thread across frameworks is the concept of "tone at the top"
  - Implies that executive management in the organization lead in a manner that sets the standards of honesty and integrity within their operations
  - Allows executive managements to demonstrate their understanding of basic internal controls by formally adopting one of these practices

Control Framework
COSO – Background

- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) produced the COSO Report providing a starting point for individual entities' assessments of internal control, for future initiatives of rule-making bodies and for education.
- COSO originally published the Report in 1992.
- COSO comprises five organizations: The IIA, AICPA, FEI, AAA, and IMA.
- The COSO framework breaks effective internal control into 5 interrelated components to simplify management's task of administering and supervising all of the activities that go into a successful internal control structure.
- As of January 21, 2002 COSO has launched a landmark new study to provide guidance in helping organizations manage risk.

Control Framework
COSO – Structure

The SEC has stated that COSO meets this requirement as it is a de facto standard adopted by many organizations.



Control Framework
COSO - Control Objectives

- COSO is primarily a business control model, limited to three primary IT areas:
  - Strategic planning
  - System design, implementation, and security
  - Business continuity
- Examples of COSO information system control objectives include:
  - Use information technology (IT) to carry out the entity's strategic plans
  - Capture, process, and maintain information completely and accurately, and provide it to the appropriate people to enable them to carry out their responsibilities
  - Make information systems available, as needed

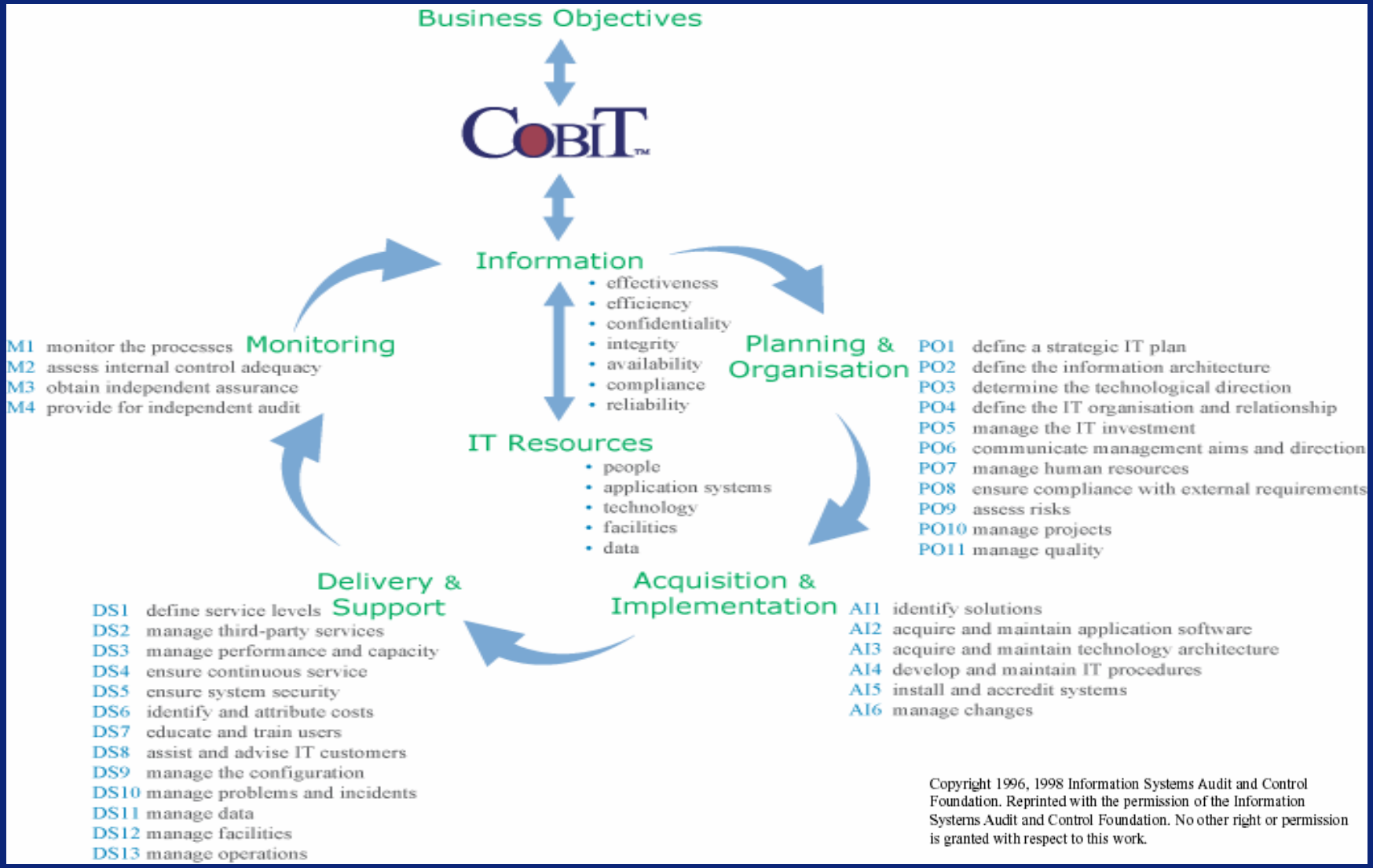
Control Framework
COSO – General Feedback

- The IT industry has changed dramatically in the past 11 years, but COSO IT controls have remained the same.
- Most organizations feel that the IT-related control activities are outdated.
- COSO offers few IT-related control activities.
- The IT-related control activities offered are extremely generic.
- There are IT-related control objectives outside the scope of the "Manage Information Technology" activity that make it challenging to plan IT audits effectively.
- Most large companies implementing COSO consider the use of alternative frameworks to identify relevant IT controls:
  - COBIT – focuses on controls over IT in support of business objectives
  - ISO 17799 – focuses on Information Security controls

Control Framework
COBIT - Background

- Control Objectives for Information and Related Technology (COBIT).
- Initially established by the IT Governance Institute in 1996.
- "(I)ntended to be ***the*** IT governance tool that helps in understanding and managing the risks associated with information and related IT."
  - – COBIT Executive Summary, 2nd Edition
- Main objective is the development of clear policies and good practices for security and control in IT, for endorsement by commercial, governmental, and professional organizations worldwide.

Control Framework
COBIT - Structure



Control Framework
COBIT - Control Objectives

- Focus on controls over IT in support of business objectives.
- Example control objectives include:
  - Management of the information services function should ensure that the continuous scheduling of jobs, processes and tasks is organized into the most efficient sequence, maximizing throughput utilization, to meet the objectives set in service level agreements.
  - Management should implement a process to ensure that the performance of information technology resources is continuously monitored and exceptions are reported in a timely and comprehensive manner.

Control Framework
COBIT – General Feedback

- COBIT attempts to bridge the gap between IT controls and the business process controls of other internal control frameworks.
- The new management guidelines component of the framework helps to address the 'how to do it' component that other standards may miss (specifically ISO17799).
- There is an effort under way to map COBIT controls to ISO17799.

Some auditors have found that the IT Governance Institute's *COBIT: Control Objectives for Information and Related Technology* aligns well with their Sarbanes-Oxley compliance efforts. The institute's *IT Control Objectives for Sarbanes-Oxley* further clarifies CobiT's relevance to Sarbanes-Oxley projects and reveals a high concentration of IT processes around COSO's "control activities" and "information and communication" components.

~*Sarbanes-Oxley: The IT Dimension.* Sally Chan, IT Audit Forum of the IIA, Volume 7, May 1, 2004.

Control Framework
ISO17799 - Background

- Considered the most widely recognized security standard
- Based upon British Standard (BS) 7799, last published in May 1999
- Has comprehensive scope and breadth and comprises best practice security processes
- Allows organizations to become ISO17799 certified
  - Providing a certain level of comfort to corporate executives and the general public regarding the overall state of security within an organization
- Can be a significant undertaking to implement
- Designed for any size organization

Control Framework
ISO17799 - Structure

- 10 major sections covering different areas of information security:
  - Business Continuity Planning
  - System Access Control
  - System Development and Maintenance
  - Physical and Environmental Security
  - Compliance
  - Personnel Security
  - Security Organization
  - Computer and Network Management
  - Asset Classification and Control
  - Security Policy

Control Framework
ISO7999 - Control Objectives

Objectives are very broad, but provide detail regarding key components that should be included:

- Information Security Architecture
  - To manage information security within the organization
  - To maintain the security of organizational information processing facilities and information assets accessed by third parties
- Security Policy
  - To provide management direction and support for information security
- Asset Classification and Control
  - To maintain appropriate protection of organizational assets
  - To ensure that information assets receive an appropriate level of protection

Control Framework
ISO17799 – General Feedback

- Several nations have indicated that portions of ISO17799 conflict with their national laws, particularly covering privacy.
- Widely used in the United Kingdom and Pacific Rim, ISO 17799 still hasn't gained traction in the United States.
- United States interest could change based on the recent CyberSecurity report.

"It's not perfect," says Giga Information Group Research Director Michael Rasmussen, "but it's the most widely adopted. You can follow other best practices, but this puts everything together in one spot, and it's internationally recognized. Wherever I go, people are asking about it."

~GuidingLITE, CSO Magazine, March 2003

General Areas of Risk

- Immeasurable
  - While strategy and plans have been documented, a clear manner of measuring progress against them was not identified and established.
- Outdated or non-existent
  - The existing strategy and plans have not been updated or evaluated in several years.
  - Based on changes in technology or management, they may no longer be applicable.
- Impractical
  - Strategies and plans established are so far-reaching they are unachievable within the defined period.

Areas of General Computer Controls
Information Resource Strategy and Planning

Controls that ensure that information systems goals support the overall goals of the organization.

-Information Systems Short and Long Term Goals

Short Term: measurable, detailed budgets, updated to track progress

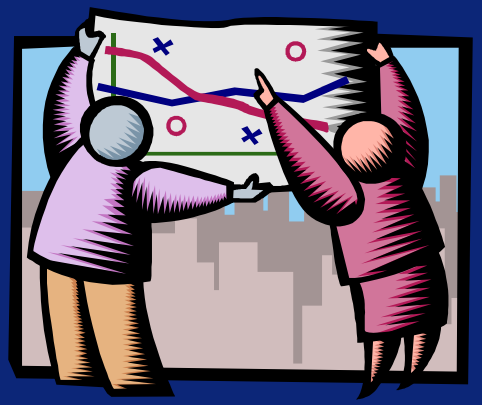
Long Term: defines information systems architecture of the organization, consistent with business goals

-Staffing of Computer Processing Environment

-IT personnel hiring procedures, performance appraisal

-IT Personnel Training

-Formal or on-the-job training



General Areas of Risk

- Lack of training
  - Team members are not adequately trained on use of information processing and IT security systems.
  - Errors and irregularities are not identified as a result.
- No follow-up
  - Errors and irregularities are identified, but no action is taken to address them.
  - Issues are recorded but never closed.
- Unsupportive management
  - While errors and irregularities are identified, persons responsible for enforcement or correction do not have the necessary support to address them.
  - Management does not acknowledge the errors and irregularities identified.
  - Management does not recognize security as a part of support and operations of IT systems.

Areas of General Computer Controls
Information Systems Operations

Controls that ensure that batch or on-line transaction process to normal completion in a timely manner and are authorized

- Monitoring of Processing and Exceptions Resolution
  - Completion of jobs is monitored
  - Exceptions are recorded and proper follow up is performed
  - Failed jobs are re-run
- Validity of Executed Jobs
  - Automated scheduling tools
  - Completion of jobs is monitored
  - Access to schedule, execute, modify production schedule and scheduled jobs is limited

Areas of General Computer Controls
Information Systems Operations (Cont.)

- Data Retention
  - Backups are scheduled and reviewed
  - Data Retention policies have been defined
  - Backups are stored in a secured location and are properly marked
  - Backups are stored off-site
- Computer Processing Environment Service Levels
  - Monitoring of performance of Computer Processing Environment
- User Training and Support
  - Users are trained to use production applications
  - Application documentation exists
  - Help Desk: review and analysis of user requests

General Areas of Risks

- No prior identification of risks
  - Management should conduct a risk assessment to identify risks associated with entering into an outsourcing arrangement prior to initiating
  - Inappropriate decisions are often the result of poor procedures for selecting outside service providers
  - Critical data accessible to non-employees
  - Potential for violation of privacy laws
  - Provides opportunities for fraud
- Bad contracts
  - Contracts may not include such things as security considerations, cancellation clauses, and status reporting requirements
- Impact of outsourced activities on accounting processes
  - Outside service providers may not understand change control processes and necessary IT policies and procedures, and may affect critical accounting deadlines and processes (for example, payroll)

Areas of General Computer Controls Relationship with Outsourced Vendors

Controls that ensure that activities performed by an outsourced vendor meet managements expectations.

- Selection of Outsourced Vendors
  - Selection criteria has been defined
  - Outsourced vendors are approved
  - Appraisal criteria has been defined
- Outsourced Vendor Service Level Appraisal
  - Vendor performance is monitored
  - Service level is appraised periodically

General Areas of Risk

- Unidentified systems or access
  - Business units are able to implement new systems without approval or oversight
  - Key corporate data can be exposed unintentionally.
  - Reports to monitor either do not exist or are too cumbersome to print and use
- Lack of an overlying security strategy
  - If an overall plan and support do not exist, individual security policies related to information security are difficult to create and administer

Another great way to identify risks within a particular area is to gather existing reports related to recent regulatory or external audits Review the descriptions, findings, resolution steps, and status of open items prior to any discussions with the business unit or to conducting tests.

General Areas of Risk

- Decentralized or loosely organized security functions
  - Can lead to lack of accountability in which every manager is responsible for security, but there is no accountability to a larger organization
  - May result in a lack of incentive to prioritize security needs over operational or financial needs
- Unusual facilities or business operations
  - Organization doesn't want to focus on security because it could hinder its customer focus.
  - Implementation of the appropriate physical or environmental controls may be considered too costly.

Areas of General Computer Controls
Information Security

Controls that define implementation and administration of access restrictions.

- Logical Access Controls
  - User access is authorized and reviewed
  - System configuration standards: passwords, lockout settings, etc.
  - Access to administer security is limited
  - Default configurations

- Physical Access Controls
  - Locks, key cards, biometrics, fence, etc.
  - Video monitoring, guards, etc.
  - Access authorization is required
  - Access is reviewed

Areas of General Computer Controls
Information Security (Cont.)

- Monitoring Controls
  - Access violation reports: failed login attempts, invalid code use, etc.
  - Access reports: data center entry log, audited files, etc.
- Anti Virus Protection
  - Software is installed
  - Virus definitions are updated
- Software Licensing Agreements
- Environmental Controls
  - UPS, A/C, raised floors, temperature and humidity monitors, etc.

General Areas of Risks

- Data loss
  - Where backup tapes are not tested, recovery may not be assured.
  - Document storage on site could be risky if physical safeguards are not in place to control access to them.
- Disruption of operations
  - The longer operations are down, the greater the impact of the disaster and the lesser the chance of the business making a healthy recovery.
- Direct expense for damages
  - If insurance and basic safeguards are not put in place and tested, the business will lose out in repairs and recovery, in addition to lost sales.

Areas of General Computer Controls
Business Continuity Planning

Controls that ensure business processes can be restored in the event of a disaster

- Business Continuity Plan
  - Business Impact Analysis
  - Disaster Recovery Plan
  - Test of Disaster Recovery Plan
- Systems and Data Backup and Retention
  - Backups are performed
  - Backups are archived off-site
  - Readability of backups is verified
  - Backups are stored in a secured, environmentally protected area.

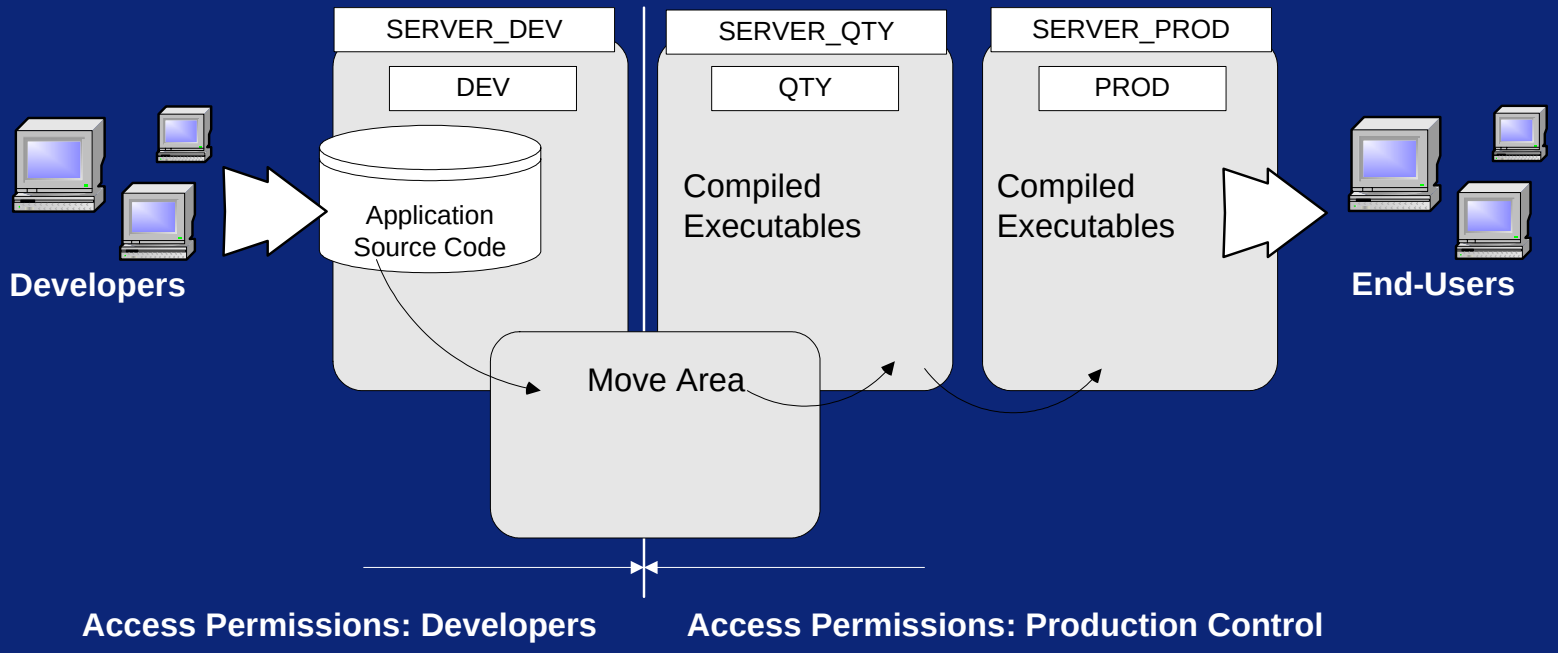
General Areas of Risks

- Cost overruns
  - Projects incur more expenses than budgeted
  - Could be due to software issues, lack of communication about allowable expenses, or poor expense monitoring
- Schedule overruns
  - Actual project end dates are later than planned project end dates
  - Often a result of poor internal design plans or functionality issues
- Delivery of less functionality than promised
  - Actual functionality does not meet expectations

Areas of General Computer Controls
Application Systems Implementation and Maintenance

Controls that ensure changes made to application systems function consistent with management expectations.

- Application Change Management



Areas of General Computer Controls
Application Systems Implementation and Maintenance

Application Change Management Process and Controls

-Change Initiation

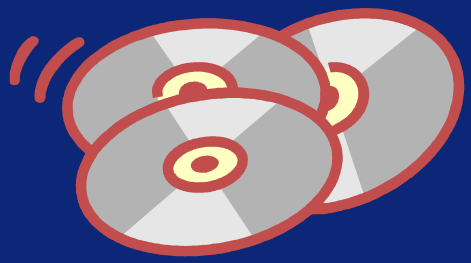
- Application changes are prioritized and approved
- Tracking of changes

- Testing of Changes

- Changes are tested: interface testing, end user testing, etc.
- Test environment separate from production environment

- Migration to Production

- Changes moved to production are approved
- Access to production environment is restricted



General Areas of Risk

- Financial misstatement
  - The database is the record of all the transactions accounted for by the company.
  - If input or processing controls render any of this information inaccurate, the credibility of the financial statements can be affected.
- Data corruption
  - The database contains master data which is the source for every transaction accounted for by the company.
  - If master data is corrupted for any reason, then each transaction using that data is invalid.

Areas of General Computer Controls
Database Implementation and Support

Database Controls

-Change Initiation

- Database changes are prioritized and approved
- Tracking of changes

- Testing of Changes

- Changes are tested: interface testing, end user testing, etc.
- Test environment separate from production environment

- Migration to Production

- Changes moved to production are approved
- Changes within production environment are logged and reviewed

Areas of General Computer Controls
Change Control – Application / Database

- Change Control Policies and Procedures
  - Change control process description
  - Application / Database development methodology
  - Data Conversions

-Source Code Maintenance
  - Source code version control
  - Documentation of the source code
  - Previous versions of the code are maintained

- Notification of Affected Parties
  - Change Management Meetings
  - Distribution Lists

General Areas of Risk

- Damaging exposure to critical systems
  - Inadvertent access to key network components can lead to malicious attacks on critical business data and systems
- Costly downtime
  - When continuing outages and errors take key networks components out of commission
- Reduced productivity
  - Due to inefficient use and maintenance of network communications software and hardware
- Access to sensitive data
  - Eavesdroppers on the network gain access to sensitive data

Areas of General Computer Controls
Network Support

- Standard Change Control Procedures
  - Initiation of changes (user requests, IT changes, etc.)
  - Testing of changes (parallel, end user, etc.)
  - Implementation of changes into production

- Network Components
  - Hubs, Routers, Firewalls, etc.
  - Server network software (Windows, Novell, etc.)

- Network Configuration Changes
  - Access control lists (firewall, router, etc.)
  - Network address changes, subnet configuration, etc.

General Areas of Risks

- Complexity
  - Software is complicated and will become even more complicated in the future due to an ever increasing amount of code.
  - This is exacerbated by the use of unsafe programming languages like C or C++.
- Extensibility
  - Modern software systems like Java and .NET are built to be extended (that is, easily updated and changed).
  - Extensibility is supported through dynamically loadable device drivers and modules.
  - Their very nature make it hard to prevent software vulnerabilities from slipping in.
- Connectivity
  - As more and more computers become connected to the Internet, the easier it is for small system failures to propagate and cause massive outages.

Areas of General Computer Controls
Systems Software Support

- Standard Change Control Procedures
  - Initiation of changes (user requests, IT changes, etc.)
  - Testing of changes (parallel, end user, etc.)
  - Implementation of changes into production

- System Software Support Areas
  - Updates and patches released by vendors: Service Packs, PTFs, etc.
  - Vendor support agreement for OS (Sun Solaris, IBM OS390, etc.)
  - Documentation of systems software configuration

General Areas of Risks

- Downtime
  - Outages can be costly to business operations, particularly, if required, replacement parts or hardware are not readily available.
- Poor performance
  - Slow processing speed and accessibility can affect business operations and increase help desk tickets and hardware team support.
- Lack of support
  - Older systems may lack the vendors and internally trained team members to be maintained effectively.

Areas of General Computer Controls
Hardware Support

- Standard Change Control Procedures
  - Initiation of changes (user requests, IT changes, etc.)
  - Testing of changes (parallel, end user, etc.)
  - Implementation of changes into production

- Hardware Support
  - Hardware acquisition
  - Manufacturer warranty
  - Vendor support agreement (Sun Solaris, IBM, Dell, etc.)
  - Documentation of hardware configuration
  - Hardware performance monitoring procedures

Member of
Deloitte Touche Tohmatsu