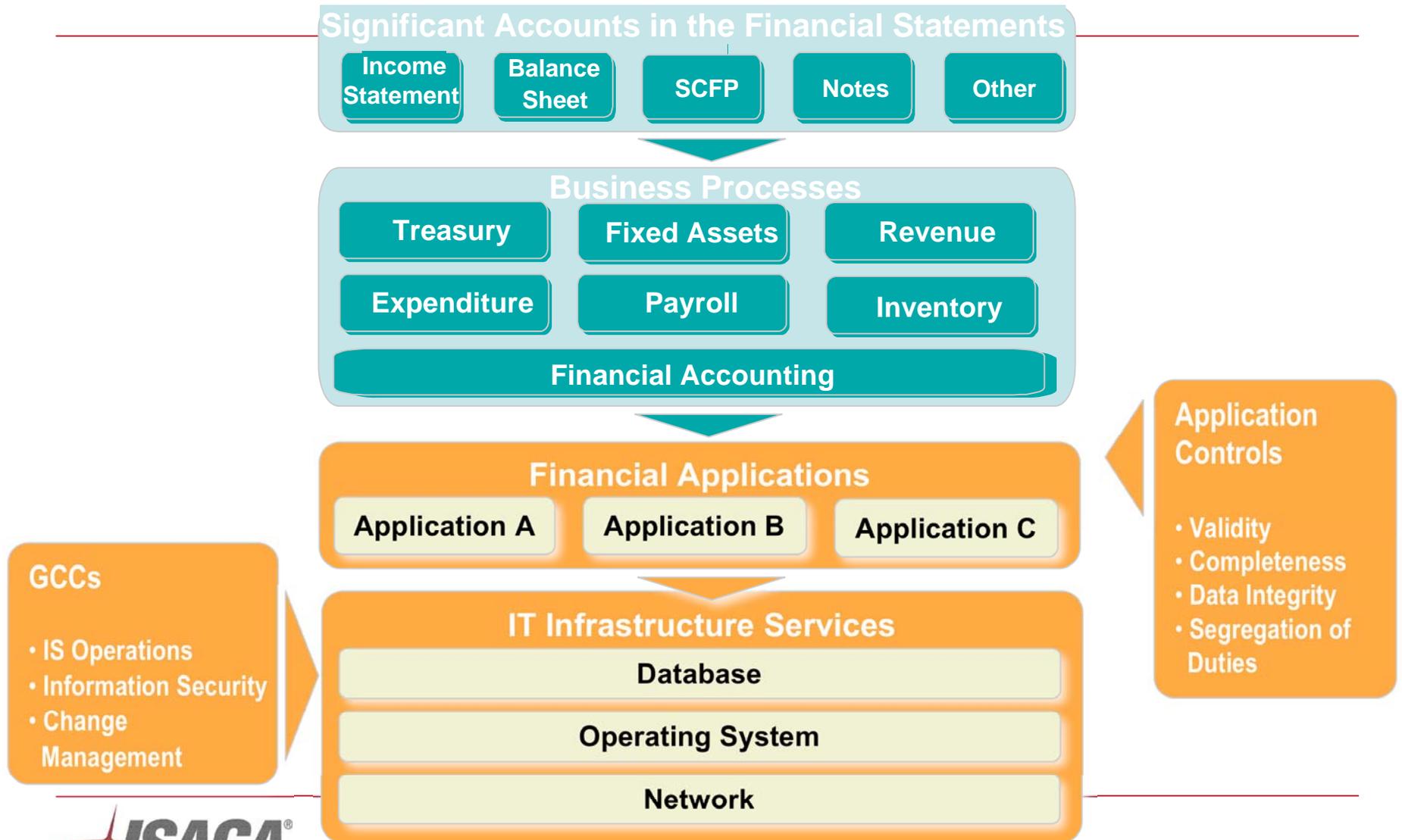# Information Systems Operations

Overview

- Operations as a part of General Computer Controls
- Key Areas of focus within Information Systems Operations
- Key operational risks
- Controls generally associated with information systems operations
- Discussion topics that can assist in initial inquiries and detailed discussions for testing information systems operations

General Computer Controls

- A ***computer processing environment*** is a computer processing location that supports a computer hardware and operating system environment.

- ***GCCs*** are controls related to the computer processing environment within which application systems are developed, maintained and operated.

- The ***objectives of GCCs*** are to ensure the proper development and implementation of applications, and to ensure the integrity of programming, data files and computer operations.

Information Security

IS Operations

Change Management
- **Application**
- **Databases**
- **Network**
- **Systems Software**

GCCs in Financial Reporting

Significant Accounts in the Financial Statements

| Income Statement | Balance Sheet | SCFP | Notes | Other |

Business Processes

| Treasury | Fixed Assets | Revenue |
| Expenditure | Payroll | Inventory |

Financial Accounting

Financial Applications

| Application A | Application B | Application C |

Application Controls

- Validity
- Completeness
- Data Integrity
- Segregation of Duties

GCCs

- IS Operations
- Information Security
- Change Management

IT Infrastructure Services

Database

Operating System

Network

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Key Areas of Focus

- Job Scheduling (sometimes referred to as Batch Jobs)
- Backup and Recovery
  - Tape backup
  - Offsite rotation of tapes
  - Recovery Testing of Tapes
- Managing Problems & Incidents
  - Helpdesk
  - Trouble tickets
- Performance Monitoring

Operational Risks

- **Inconsistent Monitoring**
  - Tools are available for scheduling but failed jobs are not consistently monitored
  - Tools are available for performance monitoring but systems are not consistently monitored
- **Unrestricted Access to Scheduling Tools**
- **No follow-up / Corrective Action**
  - Errors and irregularities are identified, but no action is taken to address them.
  - Issues are recorded but never closed.

Operational Risks

- Backups are scheduled but not monitored.
- Backup tapes are not sent offsite
- No backup tape recovery performed
- 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.

Job Scheduling

- Primary use is for time-dependent processes, such as interfaces, print jobs, backups, etc.
- On-line processing reduces the need for computer operations scheduling
- Schedule should consider job dependencies and job timing.
- Scheduling changes should be defined and controlled.

Job Scheduling

Control Objectives

- All production programs needed to process batch and on-line transactions and prepare related reports are executed timely and to normal completion.

- Only valid production programs are executed.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Job Scheduling

Control Activities examples

- Processing is monitored by management to ensure successful and timely completion, including a review and resolution of any exceptions.

- Automated scheduling tools have been implemented to ensure the authorization and completeness of the flow of processing.

Job Scheduling

Interview Topics

- Automated job scheduling system
- Access to jobs scheduling
- Process of scheduling jobs
- Evaluating dependencies
- Job Monitoring

Job Scheduling

Data Interfaces

- Need to test data interfaces
- Identify controls around interfaces
- Garbage In - Garbage Out phenomenon
- Environments may have multiple interfaces
  - Identify key interfaces
  - Evaluate materiality and risk

Backup and Recovery

- Primary purpose is to enable recovery of financial data in case of a disaster

- Types of Backup - incremental or full backups

- Frequency of backups per company policy

- Backup tapes should be stored onsite in secure location or a fire proof safe

- Backup tapes should be sent offsite

- Recovery of data from backup tapes

Backup and Recovery

Control Objective

- Data is retained in accordance with laws, regulations, and company policy to enable retrieval when needed.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Backup and Recovery

Control Activities examples

- Management and users plan and schedule backup and retention of data.

- Backups are archived off-site.

- On-going readability of backup and retained data is tested periodically through restoration or other methods.

Backup and Recovery

Interview Topics

- Tools used for backups
- Backup Schedules
- Backup Monitoring
- Backup Storage Onsite and Offsite
- Backup Recovery Procedures

Managing Problems and Incidents

- Primary purpose is to help users with system issues

- Enable smooth processing of day to day system activities

- Help Desk tools enable logging, tracking and timely closing of incidents

- Facilitates identification of training issues

Managing Problems and Incidents

Control Objective

- Users receive appropriate support to ensure that application systems function as intended.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Managing Problems and Incidents

Control Activities examples

- The help desk function acts on user queries regarding systems. Problems are recorded in a centralized problem log. Help desk personnel monitor the log to ensure a timely resolution of all such user queries.

- Management monitors problem statistics and trends to identify and eliminate root causes of recurring problems.

Managing Problems and Incidents

Interview Topics

- Help Desk Tool
- Responsibility for the help desk function
- Help Desk monitoring Issue Resolution
- Issues reporting
- Frequency of Trends analysis
- Actions taken to eliminate recurring issues

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Performance Monitoring

- Primary purpose is to monitor system performance, including capacity utilization measurement.

- Management defines service levels expectations related:

  – Availability of access to network

  – System response time

- Holding IT responsible to the user service level agreements

Performance Monitoring

Control Objective

- Computer processing environment service levels meet or exceed management's expectations.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Performance Monitoring

Control Activities examples

- Performance and capacity utilization of the computer processing environment are measured, reported, and reviewed by management.

- Management defines service level metrics. Metrics are agreed to by the affected parties.

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Performance Monitoring

Interview Topics

- Tools used for performance monitoring
- Responsibility for Performance monitoring (internally or by external vendors)
- Reports reviewed and frequency of review
- Historic performance problems
- Service level Agreements

Topics Key to SOX Audit

- Job Scheduling
- Backup and Recovery
- Operational (Value Added)
  - Performance Monitoring
  - Managing problems and Incidents.

Questions?