IT Audit

1

Dr.Lovepon Savaraj

Dr. Nongnuch Laomaneerattanaporn

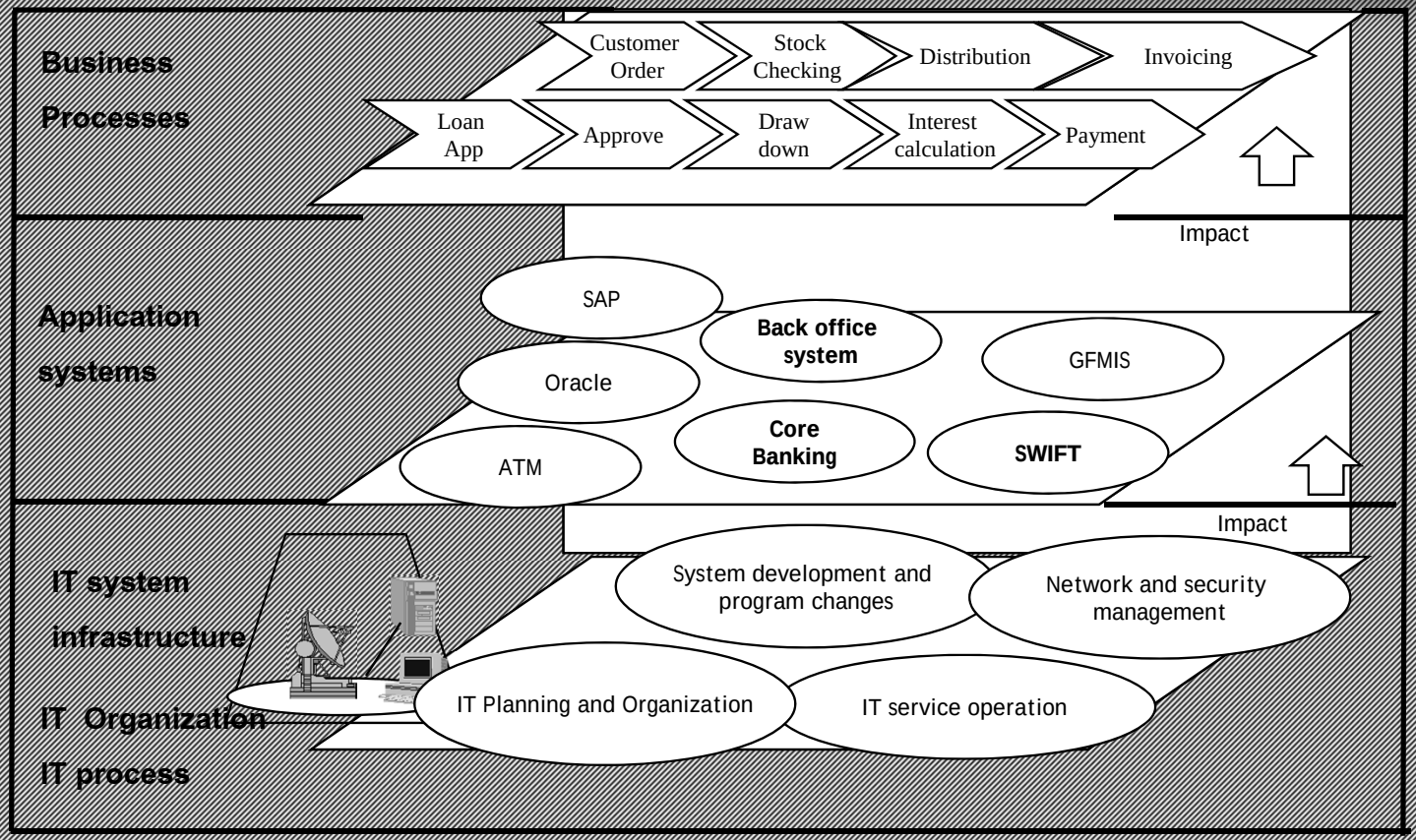
AGENDA

- Why do we need to audit IT systems?
- Type of IT controls
- IT General Controls
- Application controls

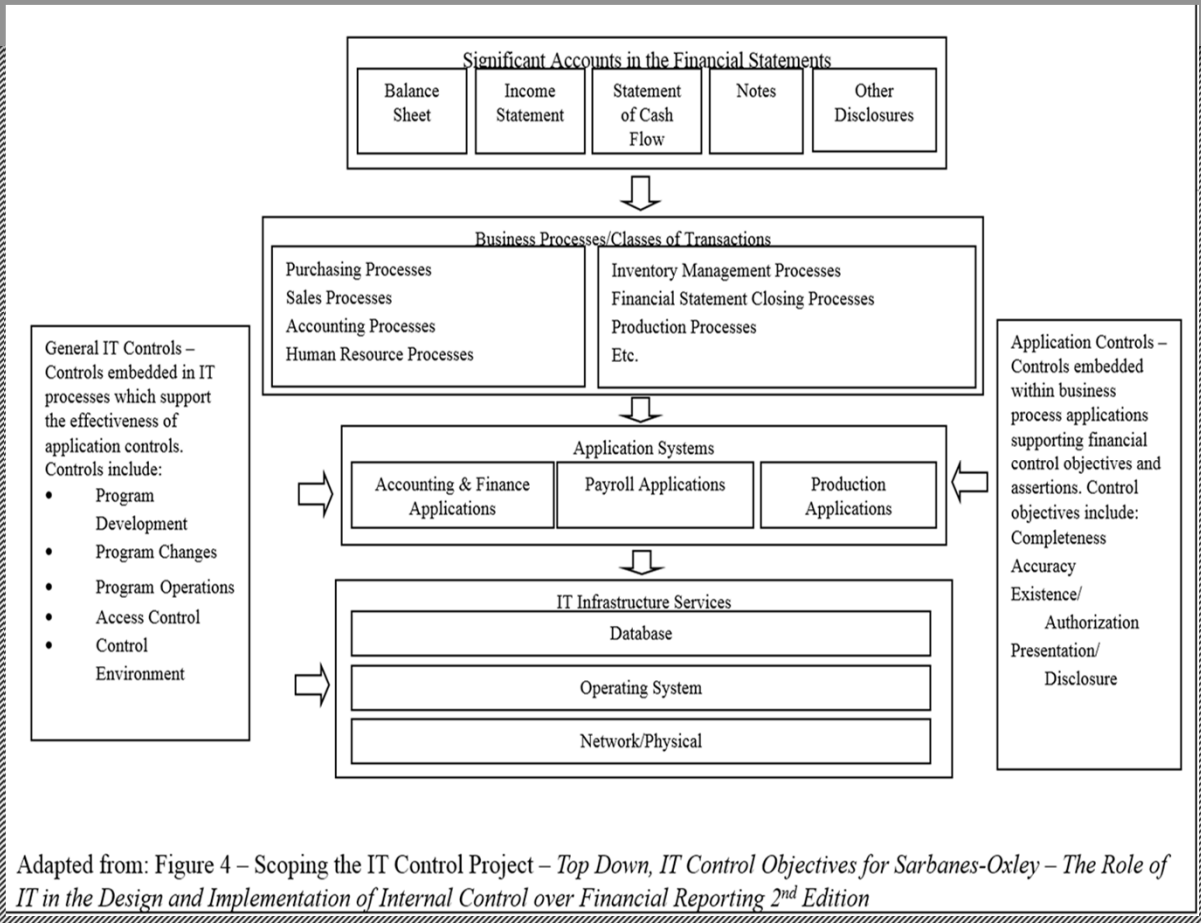
Why do we need to audit IT system?

- Highly dependent on IT system
- The companies with high overall IT risk assessment tend to have more accounting errors (Grant et al. 2008)
- Li et al. (2012) find that IT control deficiencies affect management forecasts. The management forecasts will be less accurate with the existence of material IT control deficiencies.

Why DO WE NEED To Audit IT Systems?



Why DO WE NEED To Audit IT Systems?



Adapted from: Figure 4 – Scoping the IT Control Project – *Top Down, IT Control Objectives for Sarbanes-Oxley – The Role of IT in the Design and Implementation of Internal Control over Financial Reporting 2nd Edition*

Types of IT Controls

- General controls are controls that relate to the *IT environment*, especially the environment *where application systems are developed, maintained and operated*. General controls are implemented to ensure that all automated applications are developed, implemented, and maintained properly, and in addition, that the integrity of program and data files and of computer operations are not compromised (ITGI, 2007)

- Application controls are controls that are relevant to *transactions and data* pertaining to each automated application system and are *specific to each such application*. These controls are implemented to ensure that transactions and data from both manual and automated processing are valid and completely and accurately recorded (ITGI, 2007).

Types of IT Controls

- General IT controls are *policies and procedures* used to control many applications to ensure that applications can operate effectively. These controls also include controls over IT infrastructure and processes, namely data center and network operations; system software and application system acquisition, change, and maintenance; and access security. Usually general IT controls are implemented to maintain the integrity of information and security data and to support the effective functioning of application controls. (ISA315)
- Application controls are *manual or automated procedures that are specific to each application*. These controls focus at the business process level and are deployed on the processing of transactions for each application to improve the integrity of accounting records. Application controls are relevant to procedures that are used to initiate, record, process, and report transactions or other financial data. They can be designed to be both preventive and detective controls. In short, application controls help ensure that transactions occurred, are authorized, and are completely and accurately recorded and processed (ISA315)

IT General Controls

8

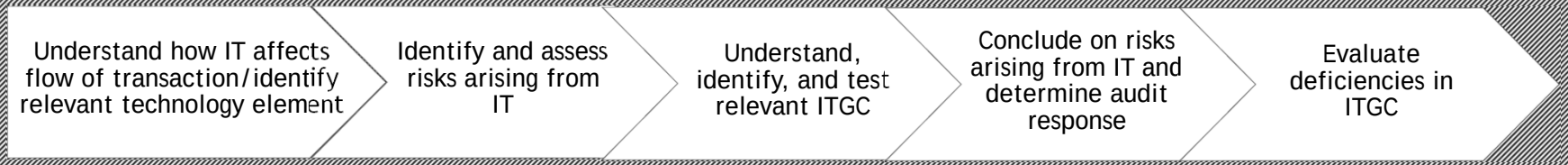
Minimum areas of ITGC controls to assess

- IT entity level control
- Application Development & Change management
- Information security
- Backup and recovery
- Third-party IT providers

(Singleton, 2010)

ITGC audit process

Illustrates the steps related to understanding how IT affects the entity's flows of transactions for significant accounts and disclosures



ITGC Elements

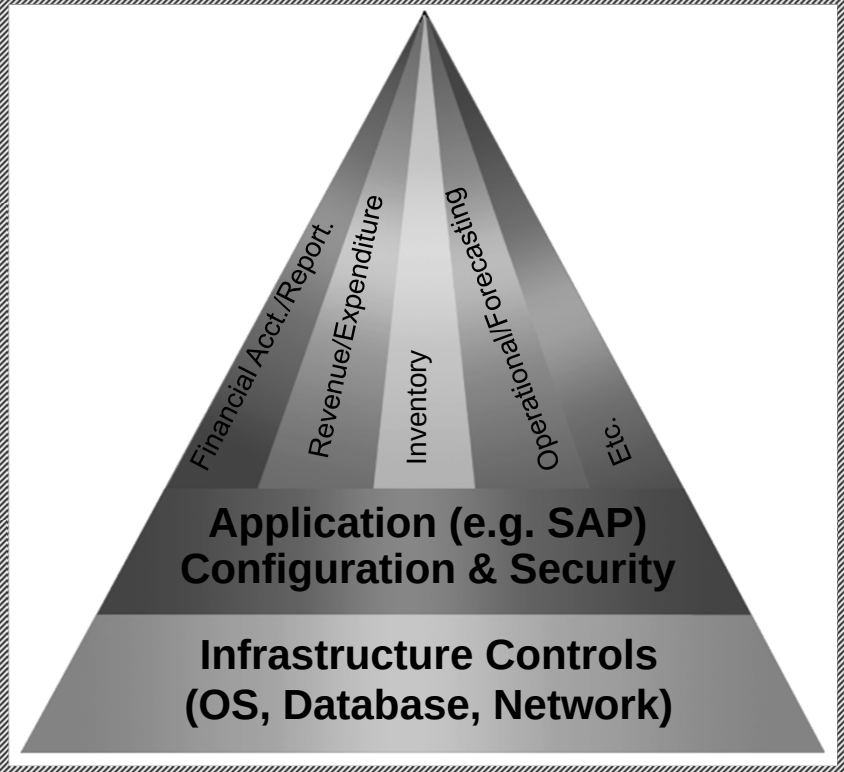
- **Application**: Interface designed to allow a user to store/retrieve data in a logical and meaningful manner and apply predefined business rules to that data. Examples include SAP, PeopleSoft, JD Edwards, Oracle, Hyperion.
- **Database**: Stores the data used by the applications. Examples include Oracle, Sybase, DB2, and SQL.
- **Operating System**: Responsible for managing communications (input/output) between hardware and applications. User authentication for many applications is dependent on operating system security. Examples include Windows, UNIX, LINUX, OS/400, and OS390.
- **Network**: A network is used to transmit data and to share information, resources and services. The network also typically establishes a layer of logical security for certain computing resources within the organization using physical devices (such as routers, firewalls) in combination with commercial software packages. Examples include Cisco, NetGear, and CheckPoint.

Relevant IT Infrastructure – Example Summary

#	Applications	Built or Purchase	Application Server Name	Application Server OS	Application Server Location	Relevant Database	Database Name(s)	Database Host Server	DB Server OS	Database Server Location	Network	App Owner – IT	App Owner – Business
1	Actual Figure Inventory System (AFIS)	Built	Z999	Mainframe	Charlotte, NC	DB2 – DSN, DSNF	AFIS DB1X I99XX9.* FFR50PRD.*	Z999	Mainframe	Charlotte, NC	AD:company.com	Dave Smith	Andy Stone
2	Sales System	Built	mssqlx1k99a\sqldb1	Windows	Charlotte, NC	SQL	FSR_External, FSR	mssql2k9cl1a	Windows	Charlotte, NC	AD:company.com	Dave Johnson	Clay Smith
3	Inventory Shrinkage Reporting (ISR)	Built	aixISRprod1	UNIX	Charlotte, NC	Oracle	ISRPRD1	aixISRprod1	UNIX	Charlotte, NC	AD:company.com	Brian Smith	Steve Jones
4	PeopleSoft Finance 8.4: Accounts Payable, General Ledger, Asset Management, Purchasing (PO)	Purchased	Z99XX Rapp1, Zapp2, & psoft999	Mainframe	Charlotte, NC	DB2 – DSNF	999PRD	Z99XX	Mainframe	Charlotte, NC	AD:company.com	Dave Johnson	Joy Li

What Can Go Wrong?

- Data is inaccurate or incomplete
- Recording of unauthorized or non-existent transactions
- Potential loss of data or inability to access data as required
- System processing is inaccurate (i.e., incorrect calculations)
- Report logic is incorrectly applying parameters
- Report logic is incorrectly gathering source data
- Unauthorized changes to systems or programs



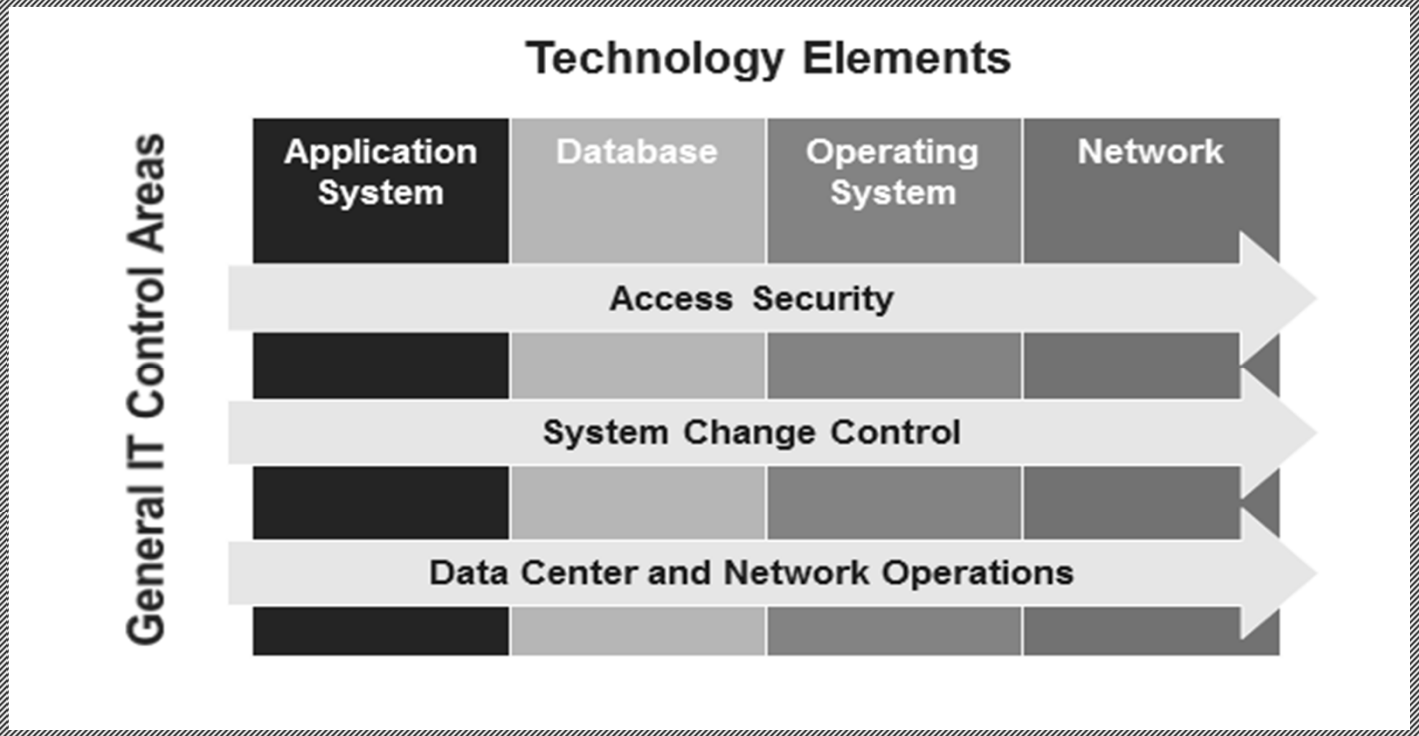
Identify ITGC Risks

PCAOB Literature	**The auditor should obtain an understanding of specific risks to a company's internal control over financial reporting resulting from IT. Examples of such risks include:** • **Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both;** • **Unauthorized access to data that might result in destruction of data or improper changes to data, including the recording of unauthorized or nonexistent transactions or inaccurate recording of transactions (particular risks might arise when multiple users access a common database);** • **The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties, thereby breaking down segregation of duties;** • **Unauthorized changes to data in master files;** • **Unauthorized changes to systems or programs;** • **Failure to make necessary changes to systems or programs;** • **Inappropriate manual intervention; and** • **Potential loss of data or inability to access data as required. [PCAOB AS 12.B4]**

Example of ITGC risks and controls

Area of IT Controls[1]	IT Risk Description	IT Risks	Technology Elements	Example Controls[2]
Access Security	User Access Privileges	Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Application; Database; Operating System; Network	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles and critical financial reporting transactions.
				AND/OR
				Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.
				AND/OR
				Access for terminated and/or transferred users is removed or modified in a timely manner in accordance with the documented company policy.
				AND/OR
				User access is periodically reviewed in accordance with the established requirements in the documented company policy.
				AND/OR
				Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.
				AND/OR
				Logging is enabled within the system, and logs are monitored or audited on a regular basis to detect unauthorized or inappropriate activity.

ITGC audit scope



Access Security

User Access Privileges	Direct Data Access	System Settings
Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Inappropriate changes are made directly to financial data through means other than application transactions.	Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users.

System Change Control

Application Changes	Database Changes	System Software	Data Conversion
Inappropriate changes are made to application systems or programs that contain relevant automated controls and/or report logic.	Inappropriate changes are made to the database structure and relationships between the data.	Inappropriate changes are made to system software (e.g., operating system, network, change-management software, access-control software).	Data conversion introduces errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data.

Data Center and Network Operations

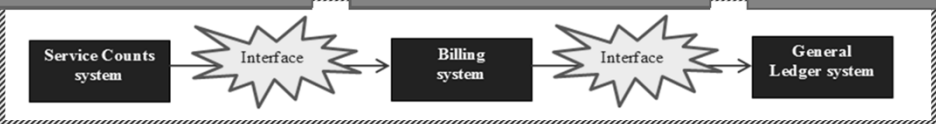
Network	Physical Security	Data Backup	Job Scheduling
The network does not adequately prevent unauthorized users from gaining inappropriate access to information systems.	Individuals gain inappropriate access to equipment in the data center and exploit such access to circumvent logical access controls and gain inappropriate access to systems.	Financial data cannot be recovered or accessed in a timely manner when there is a loss of data.	Production systems, programs, and/or jobs result in inaccurate, incomplete, or unauthorized processing of data.

System Interfaces

- Our understanding of the flow of transactions includes an understanding of the interfaces between various systems. We consider risks that data is not accurately and completely transferred.
  - System interface: Data is automatically transferred between two otherwise separate applications, typically via middleware software
  - Manual interface: Data is manually transferred from one system to another
- Identify relevant manual controls, automated interface controls, and/or general IT controls

System Interfaces (Cont'd)

Understanding	What Can Go Wrong?	Relevant Controls
Data Being Transferred	Data is not transferred accurately and completely	Manual control that is direct and precise to detect interface errors and/or Automated interface control for specific interface and/or General IT Controls if automated interface control was tested in a prior audit, refer to U.S. AAM 4161, Use of Benchmark Strategy
Source System		
Destination System		
Method of Transfer		
Frequency of Transfer		



Example of ITGC risks and controls

Area of IT Controls[1]	IT Risk Description	IT Risks	Technology Elements	Example Controls[2]
Access Security	User Access Privileges	Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties.	Application; Database; Operating System; Network	Management approves the nature and extent of user-access privileges for new and modified user access, including standard application profiles/roles and critical financial reporting transactions.
				AND/OR
				Privileged-level access (e.g., security administrators) is authorized and appropriately restricted.
				AND/OR
				Access for terminated and/or transferred users is removed or modified in a timely manner in accordance with the documented company policy.
				AND/OR
				User access is periodically reviewed in accordance with the established requirements in the documented company policy.
				AND/OR
				Segregation of duties is monitored and conflicting access is either removed or mapped to mitigating controls, which are documented and tested.
				AND/OR
				Logging is enabled within the system, and logs are monitored or audited on a regular basis to detect unauthorized or inappropriate activity.

Determine If a ITGC Deficiency Exists: Examples

Not a Control Deficiency	Control Deficiency
• The system change form for two out of 25 changes did not have documented management authorization. Alternative procedures were performed to validate the changes were authorized (corroborative inquiries and meeting minutes indicating the change was discussed and approved during management change control meeting). Refer to IC 6-15 in the Internal Control Q&As. • We tested 100% of terminated users and identified five out of 532 users that did not have their access removed timely based on the entity's policies. The deviation rate was 1% and none of the users had administrative privileges or access to modify financial transactions. Refer to IC 6-16 in the Internal Control Q&As.	• Documentary evidence indicating management reviewed access to the root account was not available for two out of five weeks selected for testing. The responsible manager was absent for two weeks and no one at the entity reviewed the access during the respective timeframe. Refer to IC 6-17 in the Internal Control Q&As. • The entity utilized one shared ID for all system changes. The password was known by multiple people within the entity and had not been changed upon initial installation. Refer to IC 6-21 in the Internal Control Q&As.

Deficiency Wording Examples

Example Control Deficiency Wording

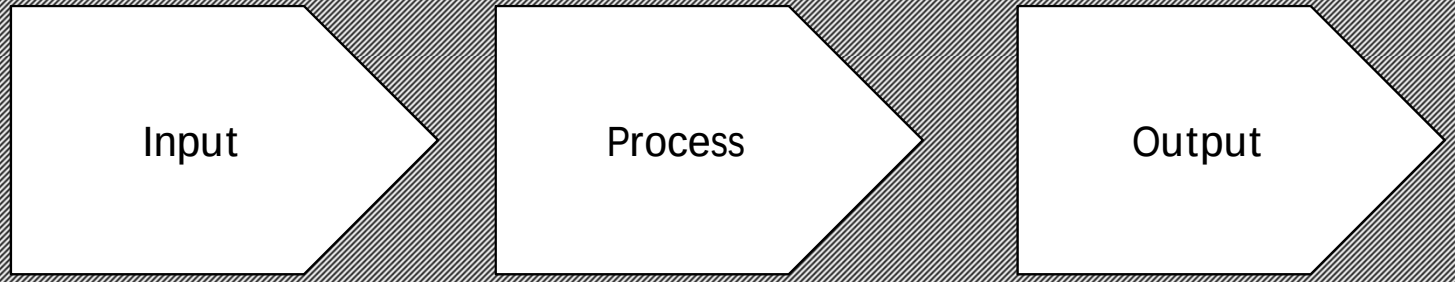
1. From a sample of 30 users, five users had access to update transactions within the MDOT system that was not commensurate with their job responsibilities.
2. A system patch applied to the Windows infrastructure environment did not have sufficient documentation to evidence approval and testing of the change prior to implementation.
3. During the semi-annual access review for the TATO system, management identified 21 users who required modification of access privileges. The related system access was not modified in a timely manner.
4. Access to bypass transaction code security is inappropriately granted to 13 users out of the total population of 65 users.
5. Certain users have inappropriate access to create or change jobs under another's user ID. Such access allows users to execute jobs and processes with elevated privileges.

Application Controls

- Application controls refer to controls over the processing of transactions and data within an application and are, therefore, specific to each application.

- To ensure the accuracy, integrity, reliability and confidentiality of the records and the validity of the entries made therein, resulting from both manual and programmed processing

Application Controls



Samples of Application Controls

Common examples of application controls include the following:

- Logical access controls (i.e., those that limit access to application functionality)
- Configurable controls (e.g., credit value limits). These are controls that can be parameterized.
- Data entry/field validations (e.g., validation of entered credit card numbers)
- Business rules
- Work flow rules (e.g., routing and sign-off of purchase requests)
- Field entries being enforced based on predefined values (e.g., pricing information)
- Work steps being enforced based on predefined status transitions (e.g., open > reviewed > closed)
- Reconciliations (manual or hybrid)
- Review and follow-up of application-generated exception reports
- Automated activity logs
- Automated calculations
- Management and audit trails (manual and hybrid application controls)

Attributes of Application Controls

- Business process controls – Control activities performed without the assistance of applications or automated systems e.g. written authorization – a signature on a check

- Automated application controls – Controls that can be programmed and embedded within an application e.g.input edit checks that validate order quantities

Attributes of Application Controls

- Hybrid controls – Controls that consist of a combination of manual and automated activities, all of which must operate for the control to be effective e.g. Shipping manager reviews a report of unshipped ordered.
  - Shipping manager reviews → Manual
  - A report of unshipped ordered → automated control

- Configurable controls – dependent on the configuration of parameters within the application system

Application Control Objectives

- Completeness – The application processes all transactions, and the resulting information is complete
- Accuracy – All transactions are processed accurately and as intended, and the resulting information is accurate
- Validity – Only valid transactions are processed, and the resulting information is valid
- Authorization – Only appropriately authorized transactions have been processed
- Segregation of duties – The application provides for and supports appropriate segregation of duties and responsibilities as defined by management

Example of Application Controls

Figure 38—Application Control Objectives for Order to Cash	
Illustrative Control Objectives	**Financial Assertions**
Orders are processed only within approved customer credit limits.	Valuation
Orders are approved by management as to prices and terms of sale.	Existence
Orders and cancellations of orders are input accurately.	Valuation
Order entry data are transferred completely and accurately to the shipping and invoicing activities.	Valuation Completeness
All orders received from customers are input and processed.	Completeness
Only valid orders are input and processed.	Existence

References

- ISACA (2014), IT Control Objectives for Sarbanes-Oxley Using COBIT 5 in the Design and Implementation of Internal Controls Over Financial Reporting, 3rd edition
- Li, C., et al. (2012). "The consequences of information technology control weaknesses on management information systems: the case of sarbanes-oxley internal control reports." MIS Quarterly **36**(1): 179-204
- Grant, G. H., et al. (2008). "The effect of IT controls on financial reporting." Managerial Auditing Journal **23**(8): 803-823.
- Singleton, T. W. (2010a). "The Minimum IT Controls to Assess in a Financial Audit (Part I)." ISACA Journal **1**.
- Singleton, T. W. (2010b). "The Minimum IT Controls to Assess in a Financial Audit (Part II)." ISACA Journal **2**.
- Hall (2011). Information Technology Auditing