KPMG

Internal Financial Controls:

IT Environment and Automated Controls

21 November 2015

Kunal Pande
Partner, KPMG

Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name, logo are registered trademarks or trademarks of KPMG International.

Agenda

1. Setting the Context
2. Risks Arising from IT
3. Understanding IT Environment
4. Application Controls
5. End-User Computing
6. Q & A

Setting the Context

Companies Act 2013 – Raising the bar on ‘Governance’

Companies Act 2013,

- **Directors** to lay down Internal Financial Controls (IFC) and ensure adequacy and operating effectiveness
- **Audit Committee** to evaluate Internal Financial Controls (IFC)
- **Independent Directors** to satisfy themselves on robust and defensible financial controls
- **Auditors** to state adequacy of IFC system and operating effectiveness

COSO 2013,

- **Codification of 17 principles** that support 5 components
- Additional guidance on **role of technology** in processes and reporting systems
- Increased insight in to the concepts of governance
- Inclusion of **internal** & **external financial** & **non-financial** reporting
- Increased emphasis on assessing and reporting to **fraud risk** and its **relationship with internal controls**

Clause 49, Listing agreement,

- **CEO/ CFO Certification:**
  - **Establish** & maintain internal **controls**
  - **Evaluate effectiveness** of the internal controls system
  - **Deficiencies** in design or operations of internal controls
  - **Steps taken** to rectify the deficiencies

Increased responsibility of key stakeholders

Need for an system around Internal Controls

Increased focus on Technology & Fraud risk

Introduction of IFC

Companies Act 2013 – Definition of Internal Financial Controls

Focus Area	Key Requirements on Internal Financial Controls	What Companies Need to do ?
Policies and procedures	• Define process and control guidelines • Assignment of responsibility, delegation of authority, segregation of duties to provide a basis for accountability and controls	• Define and disseminate policies and procedures • Develop a Delegation of Authority • Review of policies and procedures
Safeguarding of assets	• Assets and ownership interests exist at a specific date	• Assess adequacy of insurance of assets • Carry out periodic physical verification of assets
Prevention and detection of frauds and errors	• Enable proactive anti-fraud controls and a fraud risk management framework to mitigate fraud risks to the company	• Implement an Anti-fraud program. • Carry out fraud risk Assessment
Accuracy and completeness of the accounting records	• All transactions occurred during a specific period have been recorded • Assets, liability, revenue and expense components are recorded at appropriate amounts	• **Perform an assessment of:** • **Entity Level Controls** • **Process Level Controls** • **IT Controls** • **Fraud Controls**
Timely preparation of reliable financial information	• Financial items are properly described, sorted and classified • Financial information is provided as per the timelines defined by the relevant stakeholders	• Develop and disseminate accounting policy manual • Develop a robust financial close process with inbuilt controls for oversight and monitoring

A robust mechanism to report effectiveness of above mechanisms to the Board and Audit Committee is required.

Internal Financial Controls – Key Sub-elements

Processes	Strategic	Budgetary Controls & MIS, Capital Expenditure, etc.
	Operational	Order To Cash, Procure To Pay, Inventory Management, Production, etc.
	Support	Finance & Accounts, Human Resource, **Information Technology**, etc.
Risk Classification	Rating	Material / significant / control deficiencies on the basis of discussed and agreed criteria
Controls	Entity Level Controls	Code of conduct, Whistle blower policy, Transparent organization structure, HR polices, etc. This will also **include IT Entity controls**
	IT General Controls	**Base IT Controls over IT environment**
	Process Level Controls (ICOFR, OFC incl. safeguarding of assets & IT controls)	Process driven manual controls like **BRS preparation, PO creation**
		Specific **automated IT controls e.g. restricted user rights, invoice validation**
	Fraud Risk Control	Controls mitigating inherent **fraud risks** within business processes
	Categorization	**Financial Reporting**; Preventive/ Detective; Frequency;

Entity Level Controls – Key Sub-elements

Board and Audit Committee (AC) Operations

- Composition and Functional experience
- Roles and responsibilities including Agenda
- Independent Directors
- Communication to the Board/AC incl. information provided to the Board/ AC
- Board/AC oversight and monitoring
- Effectiveness Evaluation

Integrity and Ethical Values

- Code of Conduct
- Whistle Blower Mechanism
- Vendor Relations
- Customer Relations

Assignment of Authority and Responsibility

- Delegation of Authority
- Policies and Procedures
- Segregation of Duties

Organization Structure

- Organisational Structure
- Third party relationships – Legal
- Third party relationships – Investor relations
- Third party relationships – External Auditors
- Subsidiary Management

Management's Philosophy and Operating Style

- Enterprise Risk Management
- Budgeting and MIS

Financial Reporting and Disclosures

- Contingent Liabilities
- Accounting estimates
- Disclosure controls
- Notes to Accounts

Oversight and Monitoring

- Internal Audit
- Control Self Assessment
- Continuous control monitoring and assurance through data analytics/ control dashboards
- Financial review and oversight

IT Entity Controls

- **IT Strategy and Governance**
- **IT Organization and Policies**
- **IT Risk Management**
- **IT Continuity & Disaster Recovery Planning**

Risks arising from IT

Risks arising from Information Technology (IT)

IT is used to **initiate, authorize, record, process, correct as necessary, or report transactions or other financial data** for inclusion in financial statements.

IT poses specific Risks to an entity's internal control –

- Reliance on systems or programs that are **inaccurately processing data, processing inaccurate data**, or both
- **Unauthorized access to data** that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions.
- 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.

The extent and nature of these risks to ICOFR vary depending on the nature and characteristics of the company's information system.

Understanding the IT Environment

Understanding the Entity's IT Environment

IT Environment includes both the application systems and the IT infrastructure supporting those application systems, including database, operating system and network (Ref: ICAI Guidance Note relating to IFC: Section IG4.3)

The use of IT affects the way that control activities are implemented. From our perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process, and include effective Application Controls and General IT controls.

The **consideration of the IT environment include** –

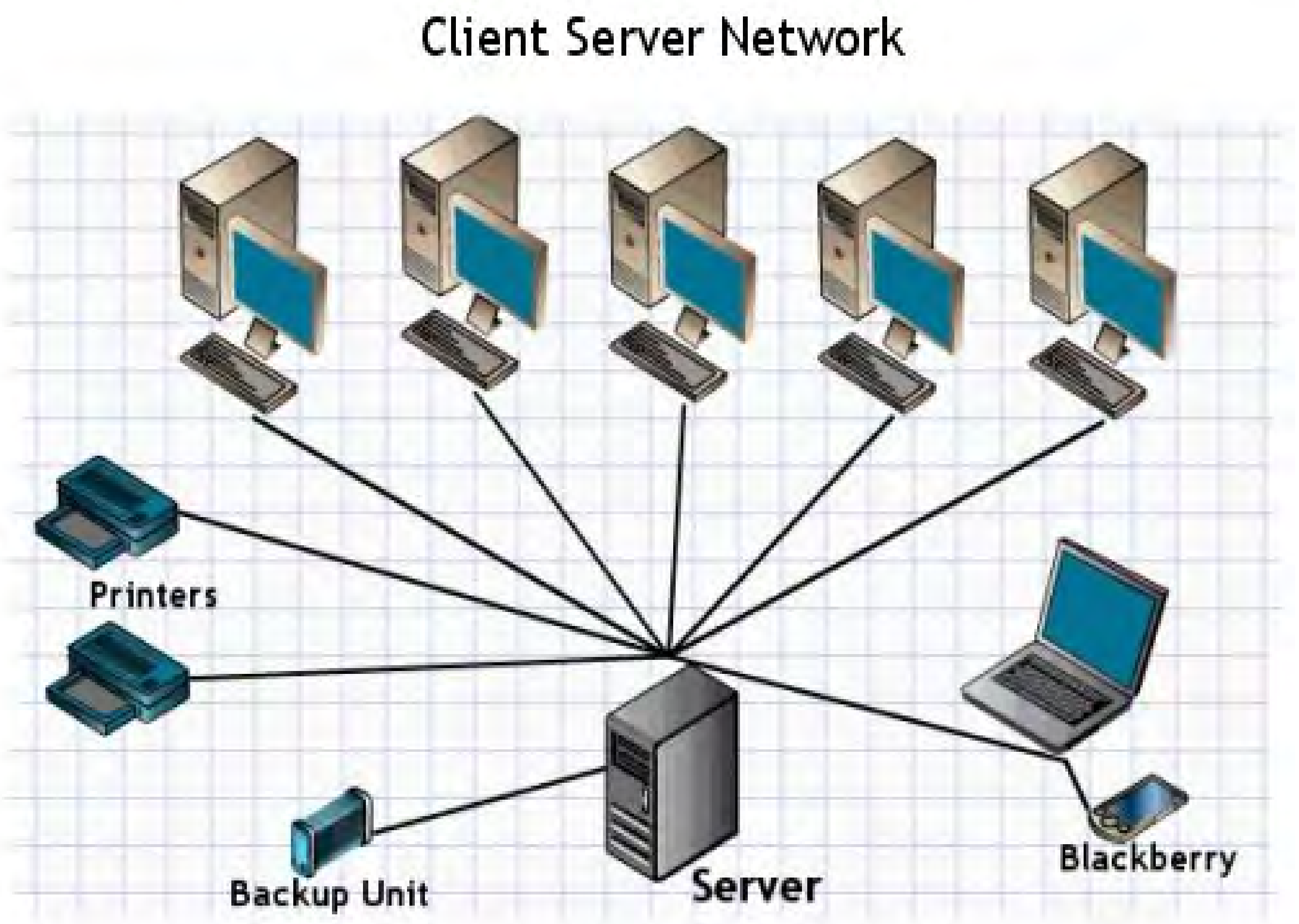
- **General description of the IT organization,** including key functions that may be outsourced
- **IT Governance Structure**
- **Nature of transactions processed** including types of information
- **Reliance on IT controls for key processes**
- **Do policies and procedures** exist to determine that IT controls are implemented in a consistent manner ?
- **Current IT Landscape** – Hardware/ Operating Systems/ Applications/ Databases/ Key business/ functions supported
- **Hosting Business Applications / Outsourcing Risks**
- **Annual IT budget** for the current year – Capex and Opex
- **How IT is internally monitored – Relevance of Internal Audit in IT**
- **Are there any significant changes** to the IT environment, including outsourcing, applications, etc.,
- **Potential risks to financial reporting arising from IT**

Understanding the Entity’s IT Environment

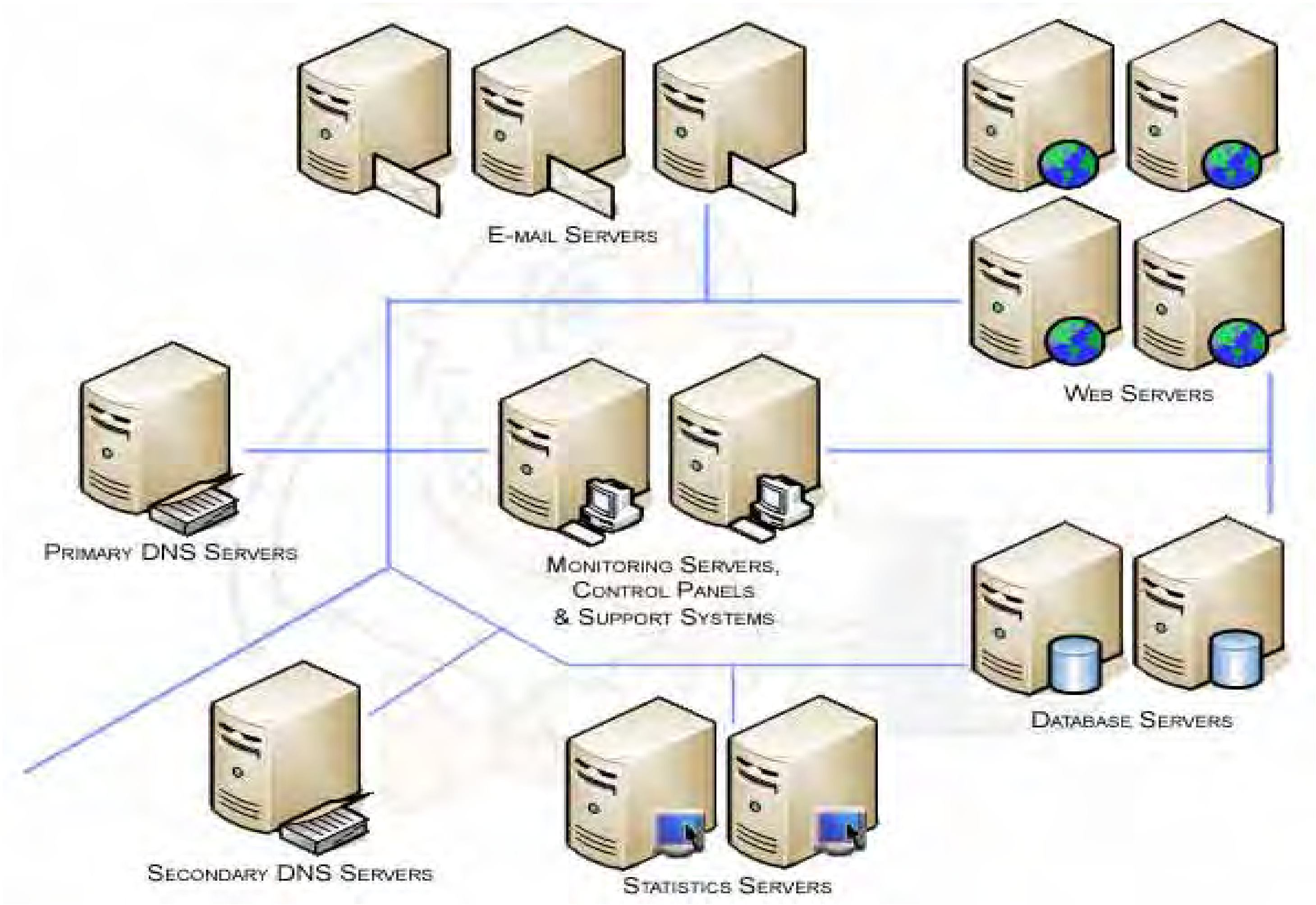
The auditor should obtain an understanding of the information system, including the related business processes relevant to financial reporting, including the following areas: (Ref: ICAI Guidance note on IFC IG 4.4)

- **The classes of transactions** in the entity’s operations that are significant to the financial statements.
- The procedures within both IT and manual systems by which those **transactions are initiated, authorized, recorded, processed, corrected as necessary**, transferred to the general ledger, and reported in the financial statements.
- **The related accounting records** supporting information and specific accounts **in the financial statements that are used to initiate, authorize, record, process, and report transactions.** This includes the correction of incorrect information and how information is transferred to the general ledger. The records may be in either manual or electronic form.
- **How the information system captures events and conditions,** other than transactions, that are significant to the financial statements.
- **The financial reporting process used to prepare the entity’s financial statements,** including significant accounting estimates and disclosures.
- **Controls surrounding journal entries,** including non-standard journal entries used to record non-recurring, unusual transactions, or adjustments.

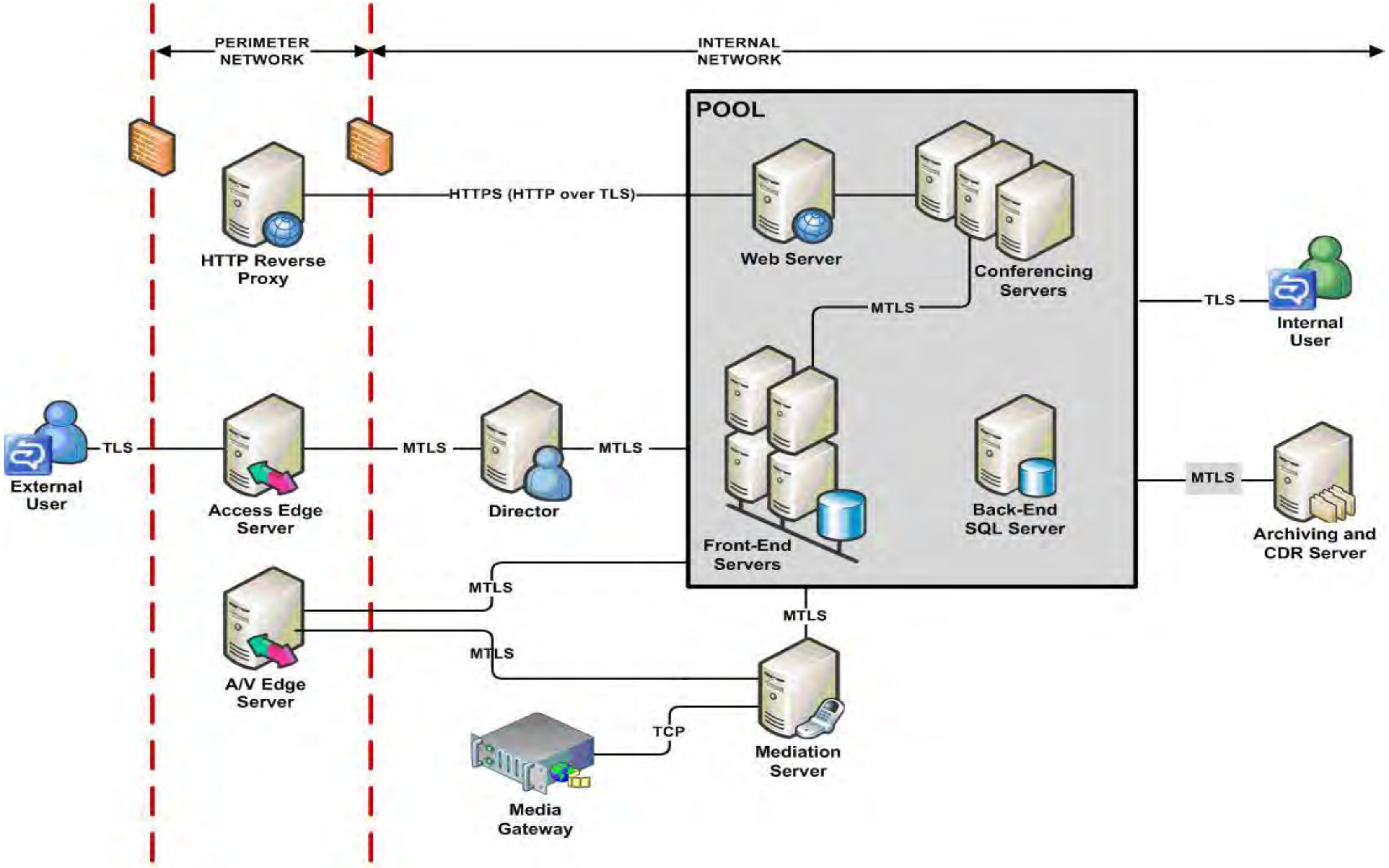
IT Environment – Examples



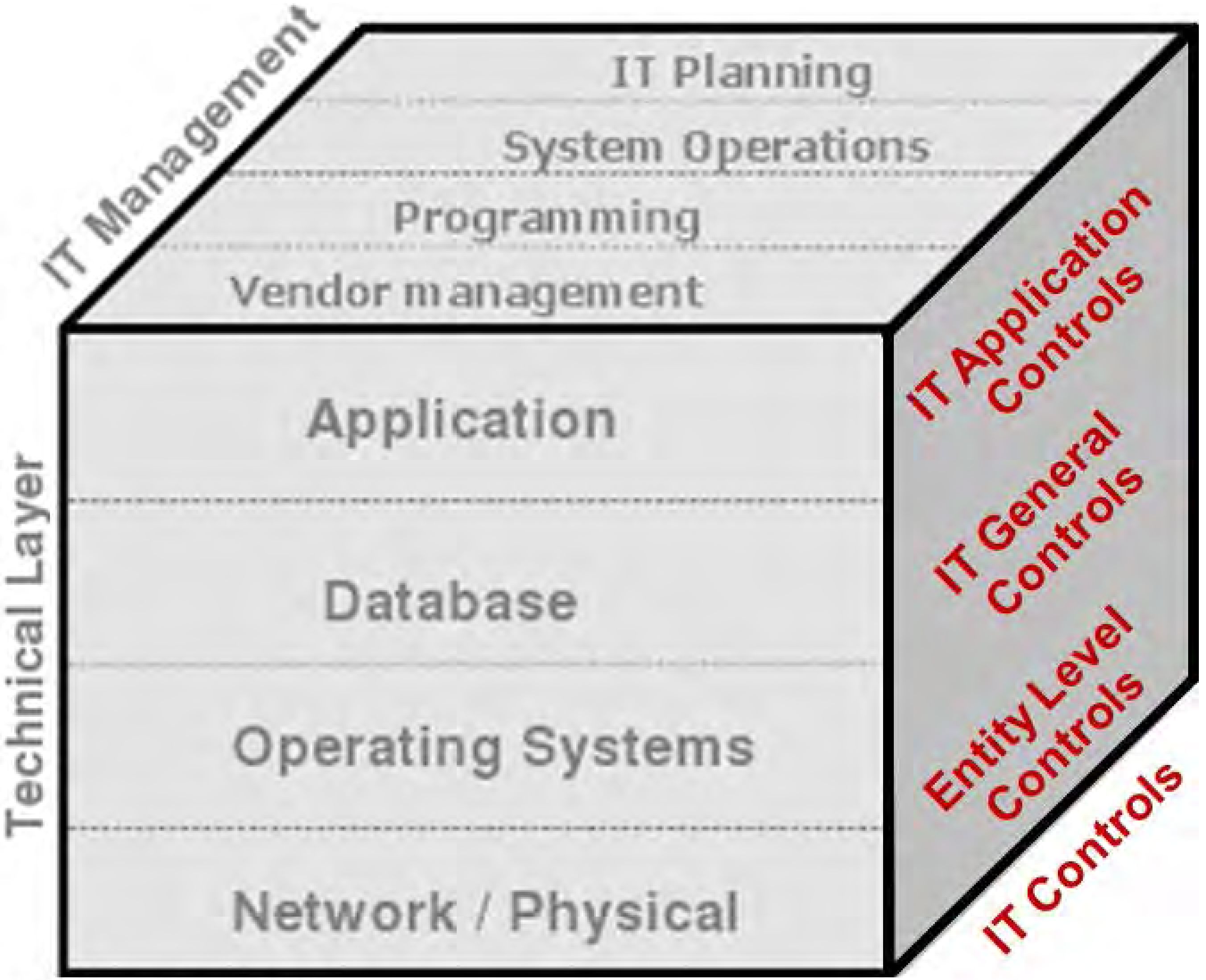
IT Environment – Examples



IT Environment – Examples



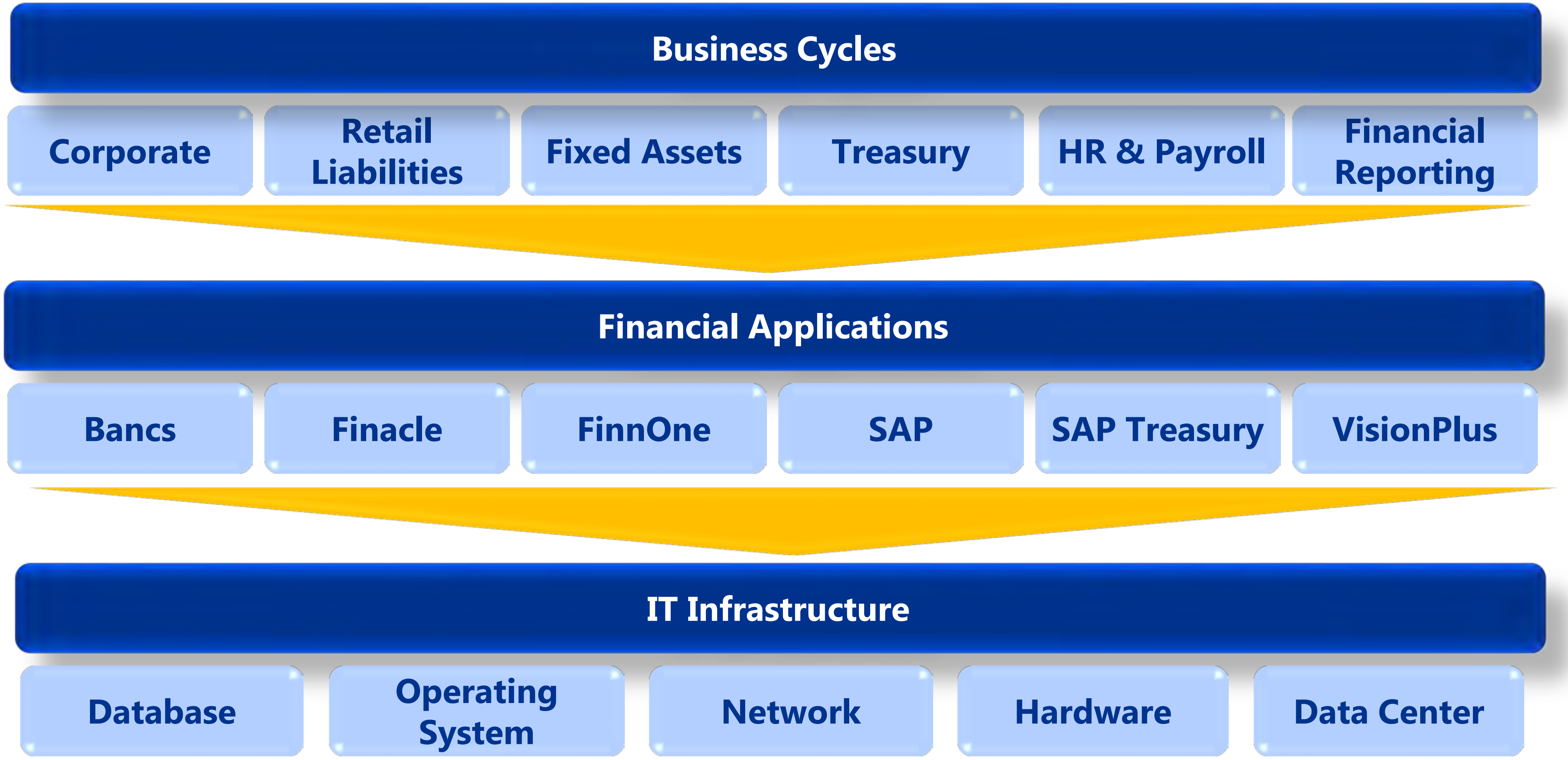
IT Landscape Simplified



Souce: Kunal Pande, KPMG

IT Environment and Financial Reporting

Relationship of IT Environment and Financial Reporting (e.g.: a Bank)



Business Cycles

Corporate | Retail Liabilities | Fixed Assets | Treasury | HR & Payroll | Financial Reporting

Financial Applications

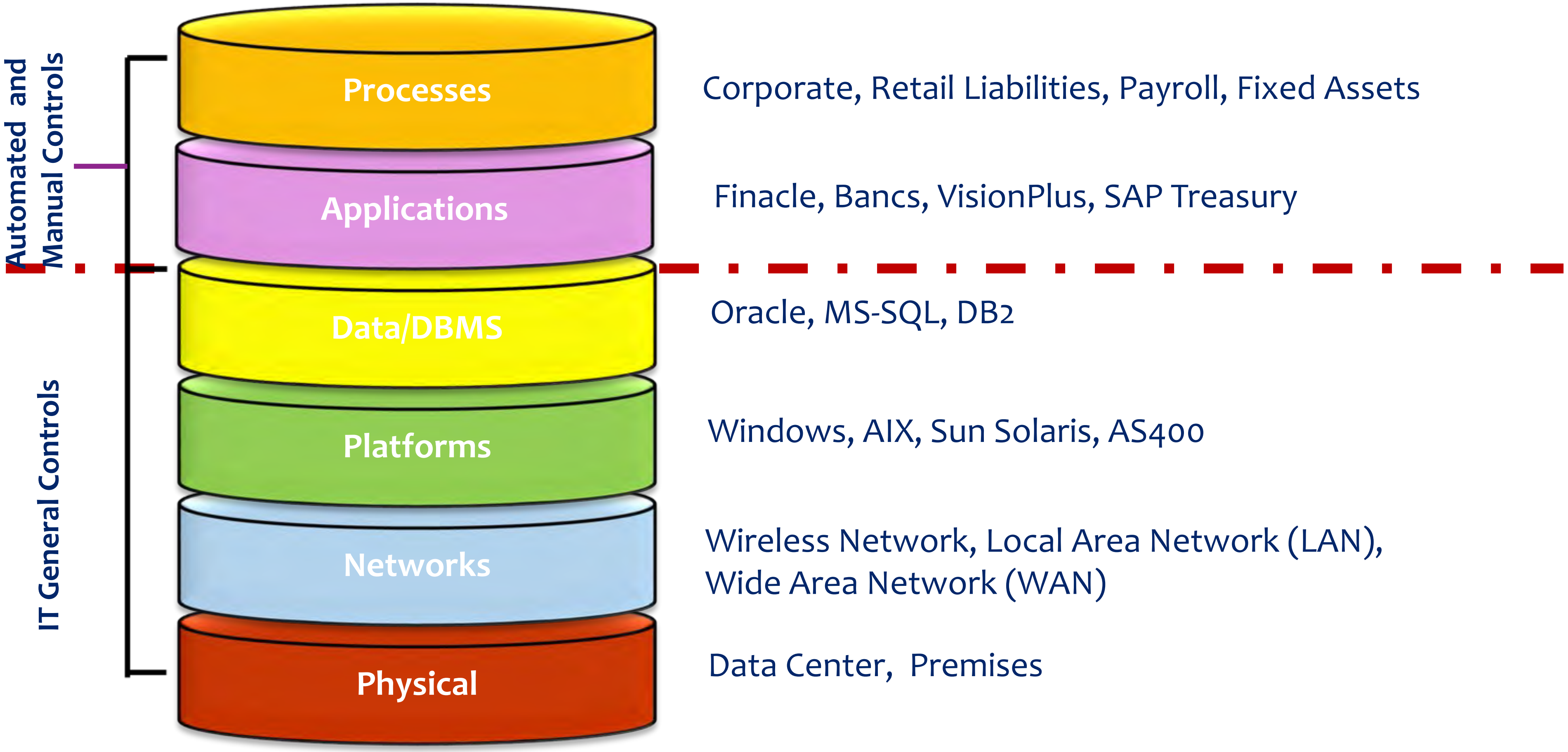
Bancs | Finacle | FinnOne | SAP | SAP Treasury | VisionPlus

IT Infrastructure

Database | Operating System | Network | Hardware | Data Center

General Security vs Application Security

- Application controls achieve process level audit objectives
- General Security Controls help us rely on application security controls



Corporate, Retail Liabilities, Payroll, Fixed Assets

Finacle, Bancs, VisionPlus, SAP Treasury

Oracle, MS-SQL, DB2

Windows, AIX, Sun Solaris, AS400

Wireless Network, Local Area Network (LAN),
Wide Area Network (WAN)

Data Center, Premises

Application Controls

Application Controls

Many control activities in an entity are partially or wholly automated using technology. These procedures are also known as automated control activities or automated controls.

Application level automated controls relate to controls embedded in systems and applications over the processes used **to initiate, authorize, record, process and report financial information**

Types of Application controls include –

- System configuration / Account mapping
- Interface controls
- Exception/edit reports, including review of these reports
- System access, including enforcing segregation of duties

Application Controls

Why are we considering the control:

- **Identify what could go wrong** and the related account balances and assertions
- Understand **how the control fits into the overall audit approach** and what we are trying to accomplish
- Have we thought through other controls in the process that address the same assertions and may be more efficient to test?
- **Is the control appropriately worded to reflect the activity, WCGW**, and process to be addresses or mitigated?

Evaluate design and implementation:

- Inquire with key stakeholders responsible for using/monitoring the automated control
- Inspect any relevant system documentation (e.g. user help files that describe the control)
- Inspect/observe the flow of transactions through the system
- Would the control, if designed, implemented, and operating effectively, prevent or detect and correct a material misstatement?

Consider GITC testing results

- Consider impact of deficiencies from GITC testing

System configuration / Account mapping controls

System configuration controls are "switches" that may be set by turning them on or off to secure data against inappropriate processing, based on the organization's business rules.

Account mapping controls are controls that relate to how a transaction is posted to the general ledger and then to the financial statements.

System configuration/account mapping controls may **include standard controls** that come with the IT application or system (e.g. the ability to enter only a valid date in a date field) **and customized controls** that are developed or changed by the entity (e.g. a parameter setting or switch to prevent the user approving a transaction over a certain amount).

Examples for system configuration controls :

- Purchase ledger clerk cannot order items over $8,000 without approval
- Date for inventory receipt cannot be posted prior to current date
- Three way match for goods receipt

Examples for account mapping controls :

- Sales coding to ensure revenue posted to correct subsidiary within group trial balance
- Posting of foreign exchange gains or losses

System configuration / Account mapping controls (Contd…)

System Configuration controls includes:

Configuration settings:

- Input, edit and validation controls
  - Input controls prevent a transaction from being processed further without all required information being input.
  - Edit controls check the accuracy of data entered into a specific field.
  - Validation controls identify data errors, incomplete or missing data and inconsistencies among related data items.
- Sequence checking
- Reconciliation configuration setting

Processing Controls

- Often occur within "batch" processing which may result in an exception reports
- Edit checks (other than input edit)
- Run-to-run totals

Calculations

- Functions that convert data using a mathematical algorithm, or an accumulation formula.

Account Mapping controls includes:

- How a transaction is posted to the general ledger
- Automated system interfaces often involve account postings to map the output from these procedures

Interface controls

Data interface is **the transfer of specifically defined portions of information (data) between computer systems.**

A data interface may be **automated, automated with a manual component or manual control.**

The **function** of a data interface control is to determine that the **data are transferred securely, once and only once, completely, accurately, and with integrity.**

Interface controls **compare data between computer systems** and may include the use of control totals, hash-totals, and/or validity checks (e.g. whether existing account numbers are used).

Types of Interfaces:

Manual:

- Typically via ASCII/text files or Excel/Access
- Subject to human error
- May be performed by the IT department – additional risk?

Automated or batched (System scheduled):

- Little or no human intervention
- Requires effective Computer Operations General IT Controls

Interface controls (Contd…)

We may **consider the following items** when evaluating the design and implementation of an interface control:

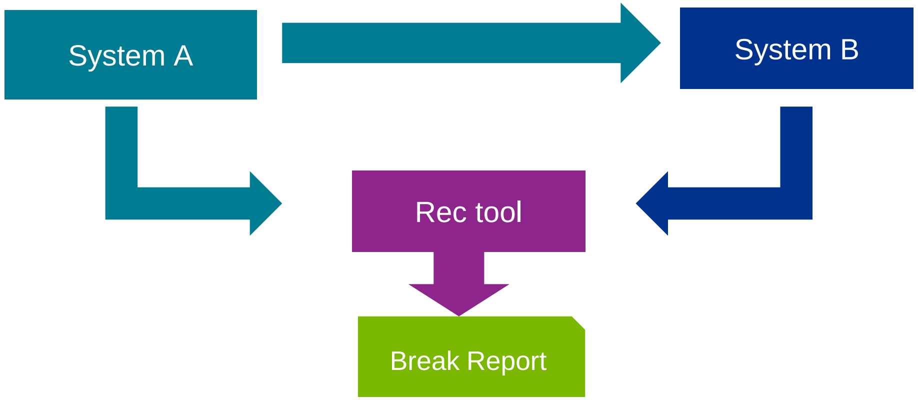
- How is the interface control **designed** to function?
- Is the interface **manual or automated**?
- Is the control the **system default or has it been customized** (i.e. standard or custom)?
- Is the interface **subject to manual intervention**?
- What **types of data are processed** by the interface control?
- What controls are in place to determine that all of the information from one system is **received completely**, and only once?

Testing Interface controls :

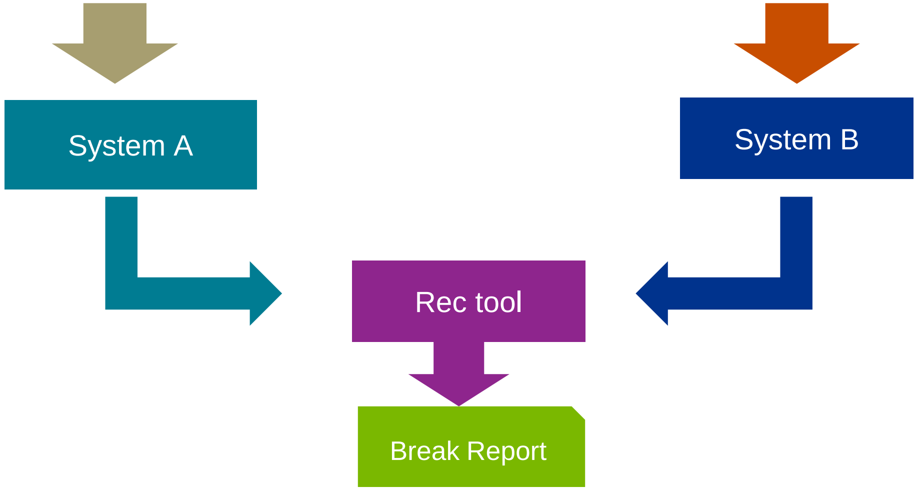
- Confirm the event that initiates operation of interface
- Confirm the extent and nature of data transferred by the interface
- Observe interface operation and obtain evidence that expected outputs from the process are accurately completed
- Reconcile batch totals / specific data between source and destination location

Testing Interfaces

C&A of the interface between two systems



C&A of the between two independent systems



Exception/edit reports

Exception/edit reports, including review of these reports –

- An exception control is **designed to identify a violation of a set standard** (e.g. customer sales exceed credit limit; three-way-match does not reconcile).
- An edit control is **designed to identify a change to a master file** (e.g. addition of a new employee; changes in wage rates).
- Exception/edit reports may **often rely on a system configuration control**. The output of the configuration control would appear on the exception/edit report.
- Designed **to verify the completeness and accuracy of information processing** and may include preliminary reports to review the accuracy and completeness of data input and control totals to verify information processing.

E.g., a configuration is set up in the IT system to perform an automated three-way-match control for purchasing invoices. If the three-way-match for the invoice does not reconcile, the exception(s) identified by the automated control are included on the exception report (e.g. unmatched invoice report) and the appropriate personnel follow up on those exception(s).

Follow-up and resolution of an exception/edit report is a manual control (the follow-up) that relies on an automated control (the report)

Exception/edit reports (Contd…)

Evaluate the design and implementation:

- How the report is generated, including the frequency of the report and the controls surrounding the generation of the report (including relevant general IT controls)?
- How management follows up on the report, including the timeliness of this follow up, if it is documented, and what corrective actions are taken?

Examples for Exception/Edit report controls :

- Extracted data to show individual sales greater than $400,000
- List of employees whose timesheets not submitted by 5pm each Friday
- Report of unbalanced journals held during month end financial reporting

System access, including enforcing segregation of duties

System access is the **ability that individual users or groups of users have access to an IT system**, as determined and defined by access rights configured in the system.

System access controls are implemented by management **to help determine that the access rights of an individual are limited in accordance with job responsibilities and business policies.** In addition, system access controls may be used **to enforce the authorization of transactions.**

System access controls are the **configuration controls to manage segregation of duties** (who is authorized by management based on his task and responsibilities to perform certain transactions) in an automated environment.

Segregation of duties means that **no single individual has control over two or more phases of a transaction or operation**

Examples for System access controls :

- A purchase ledger clerk does not have access to authorize payments.
- Sales assistants do not have access to remove blocks on customer accounts and adjust credit limits.
- Payroll clerks do not have access to adjust compensation tables.

Segregation of duties (SoD)

SoD – Key Areas to Look Out For:

- Excessive full system admin access by IT.
- Excessive system admin access by business unit personnel for user administration.
- Excessive system admin access by IT personnel limited to user administration.
- "Super User" access by IT personnel (transactions start to finish or configuration change ability).
- "Super User" access by business unit (transactions start to finish or configuration change ability).
- Too many "Super Users" override process level controls (business or IT).
- IT or business unit personnel who can change configurations without business approval.
- IT developers with access to production.
- End user or IT personnel that can process a transaction from start to finish circumventing all controls.

End-User Computing

End-User Computing

- **Processing that generally takes place on an individual’s desktop** through office automation tools (e.g., Excel spreadsheets or Access databases
- **Common in financial consolidation, reporting and disclosures** (might be considered significant application)
- Also often used for **recording non-routine business transactions** that may not be handled by transactional systems
- **Developed outside the ‘established’ IT frameworks**
- Generally **built directly by the user**
- Can be **created across a variety of platforms**
- **Developed for a variety of different purpose**

Key Risks of End-User Applications

Risk	Control process
1. Error in the calculation or processing performed of the application	Development methodology
2. Inappropriate change to the calculation or processing performed by the application	Security management
3. Understanding of the application resides with a single person so that: • unable to use the application • unable to change it	Application documentation Cross training
4. Using an old or incorrect version of the application	Change management
5. Inappropriate access to confidential information	Security management
6. Input data processed by the application is incomplete or inaccurate	Inputs and data feeds
7. Loss of information or inability to access the application	Storage and backup

EUC examples

Schedules of data supporting account balances and disclosures

- Inventory classified by Raw Materials, Work in Process and Finished Goods
- The detail of fixed assets by type, such as Land, Buildings, Equipment, Furniture & Fixtures
- Calculations of KPI Information reviewed by management as a control
- Sales volumes by customer
- Tax calculations, derivatives, calculating inventory turns, financial consolidation, etc.
- An access database that is queried several different ways to provide disclosure information, such as the classification of loans at a bank by balances, average interest rates, delinquencies, etc.

Questions & Answers

THANK YOU

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Kunal Pande

Partner
Advisory Services

Lodha Excelus,
Apollo Mills compound,
N.M Joshi Marg,
Mumbai – 400 011, India

Cell: +91 98926 00676

Email: kpande@kpmg.com