Electronic Audit Evidence (EAE) and Application Controls

Tulsa ISACA Chapter

December 11, 2014

EY

Building a better working world

Agenda

- Recent IT-related PCAOB inspection themes:
  - Internal control over financial reporting
  - Multi-location scoping
  - Consideration of IT systems, including related EAE
  - Range in substantive areas including revenues, inventory, internal use software, intangible assets, loans and ALL
  - Additional impact as to significant risks, including fraud risk, procedures and EQR
- Electronic Audit Evidence (EAE)
- Application Controls
- Questions

Electronic Audit Evidence (EAE)

What constitutes EAE

- **Definition:** *Electronic audit evidence (EAE) is data generated or processed through an IT application, and/or end user computing solution (e.g., Excel, data warehouse tools, slide decks), be it in electronic or printed form, used to support audit procedures*
- **Types:**
  - Data supporting the performance of internal controls, including key performance indicators
  - Data that represents substantive audit evidence to support assertions for significant accounts
  - Other data provided by the entity

*The **majority** of the audit evidence we receive to support the execution of our tests of controls and substantive procedures is considered EAE.*

Data supporting the performance of internal controls, including key performance indicators

- Represents data and reports used by management to:
  - Identify and investigate transactions or occurrences that do not meet business requirements or thresholds
  - Review the appropriateness of recorded transactions
  - Reconcile balances between sub-ledgers and the general ledger
  - Assess and support the validity and accuracy of inputs used in calculations
  - Monitor the company's overall performance
- Review controls over estimates and non-routine areas typically rely on data or reports that would be considered EAE
- Examples

Data that represents substantive audit evidence to support assertions for significant accounts

- Data or reports used in our substantive testing procedures
- Consists of both financial and non-financial data that we use to:
  - Perform substantive analytics
  - Substantiate and support account balances and variance explanations
  - Evaluate estimates and forecasts
- Examples

Other data provided by the entity

- Data or reports used to select our samples for tests of controls and substantive testing (e.g., population listings)
- Examples

Other key considerations

- EAE is relevant to all professionals who support the audit
- Our responsibilities for identifying and evaluating EAE is applicable to all EAE used in our audit procedures, including those related to accounts not affected by significant risks
- EAE can be applicable for both our tests of controls and substantive procedures.

Since the requirements for evaluating EAE may differ (e.g., integrated audit vs. non-integrated audit), it is critical that we appropriately understand the use of the EAE in our audit procedures

Requirements over evaluating EAE

EAE strategy

Use of EAE	Integrated audit	Non-integrated audit
Test of controls **(Data and reports used by management in the performance of controls)**	Evaluate and test controls over the completeness and accuracy of data and reports	One of the following for each piece of EAE: ► Directly Testing EAE ► Tests of Direct Controls ► Benchmarking
Substantive testing	One of the following for each piece of EAE: ► Directly testing EAE ► Tests of direct controls ► Benchmarking	

EAE Strategy (cont.)

Integrated audit

- *When using information produced by the company as audit evidence, the auditor should evaluate whether the information is sufficient and appropriate for purposes of the audit by performing procedures to:*
  - *Test the accuracy and completeness of the information, or test the controls over the accuracy and completeness of that information; and*
  - *Evaluate whether the information is sufficiently precise and detailed for purposes of the audit" (PCAOB AS 15.10)*
- ***"…the effectiveness of a control cannot be inferred from the absence of misstatements detected by substantive procedures…" (PCAOB AS 5 B9)***

Non-integrated audit

- *When using information produced by the entity, the auditor should evaluate whether the information is sufficiently reliable for the auditor's purposes, including, as necessary, in the following circumstances:*
  - *Obtaining audit evidence about the accuracy and completeness of the information*
  - *Evaluating whether the information is sufficiently precise and detailed for the auditor's purposes (AICPA AU-C 500.09)*

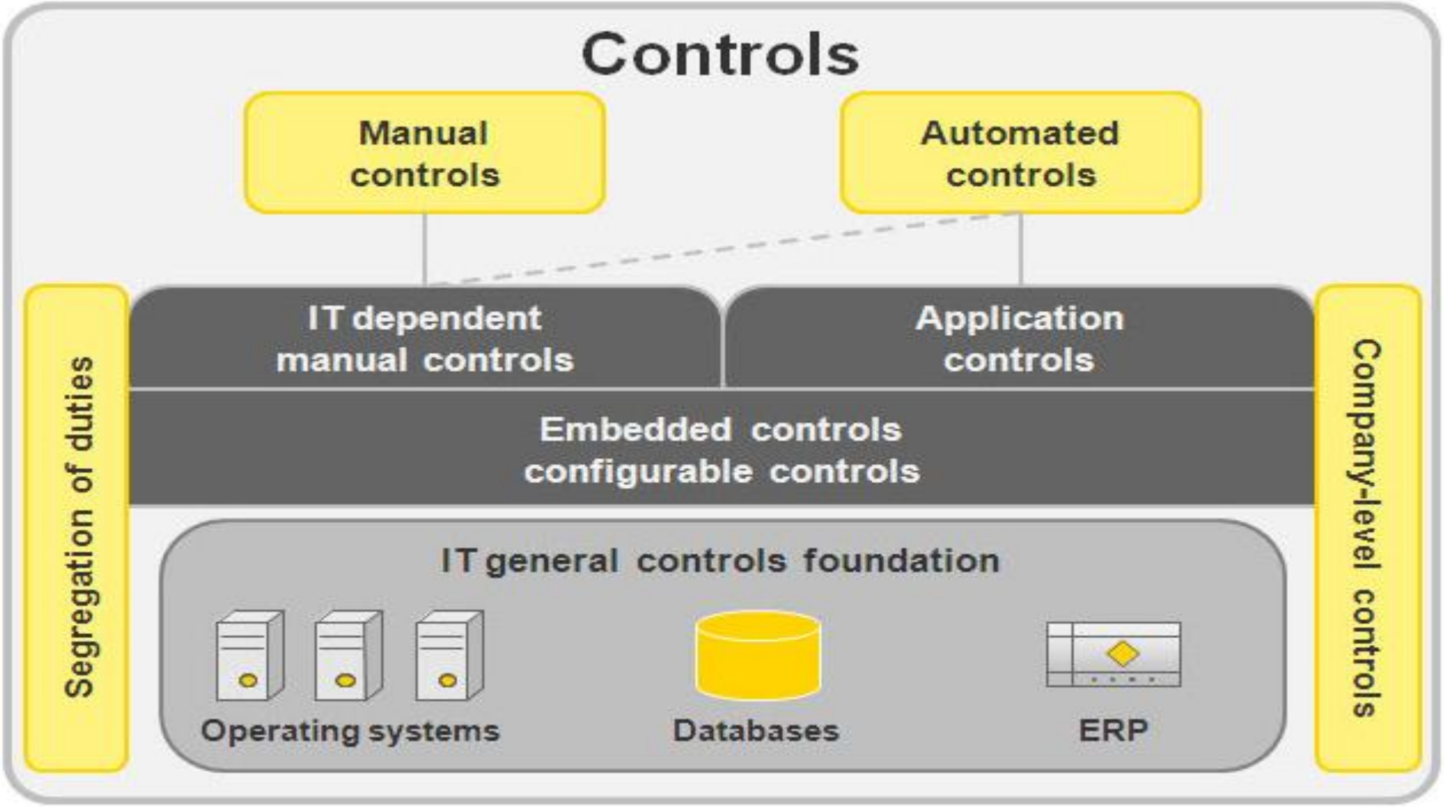
End-user computing solutions

- End-user computing solutions likely are not subject to IT-general controls
  - Excel files
  - Access databases
  - Dynamic data warehouse reporting tools
  - System-generated data in slide decks
- Need to better consider issuer controls over end-user computing solutions
  - Input control – the company reconciles data back to source documents.
  - Access controls – Access is restricted to authorized personnel and is password protected
  - Version control – Standard naming conventions are in place so only current and approved versions are used

Application Controls

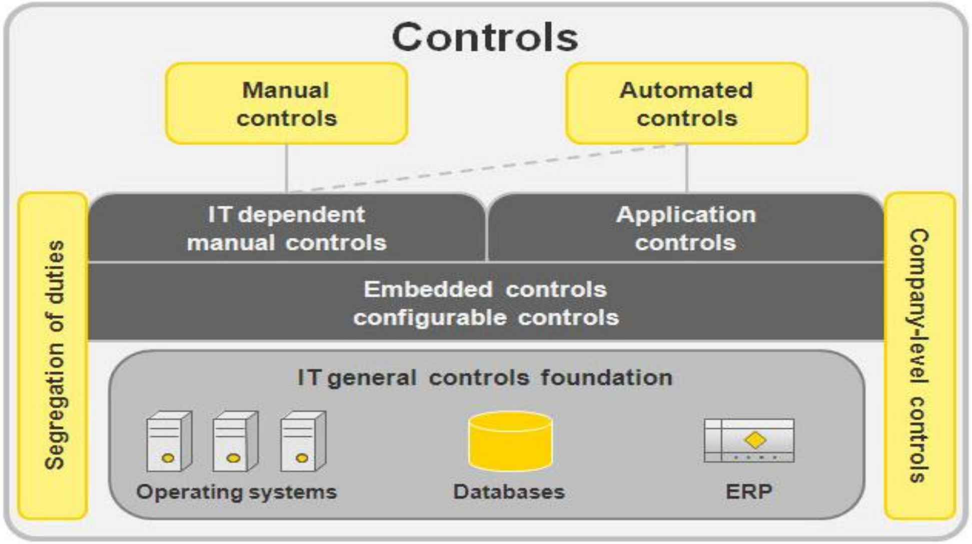
Classification of controls

- The diagram below illustrates the automated aspect of controls in an IT environment
- There are two categories of automated aspects of controls: IT-dependent manual controls and application controls



What are application controls?

- Automated functionality within the system that affects the processing of transactions
- Can be characterized as either embedded or configurable
  - **Embedded –** functionality is programmed within the application code
  - **Configurable –** functionality depends on key settings and fields within the application
- Often more effective than manual controls
- “Test of one” strategy (of each scenario) may be sufficient with effective IT general controls



Application control categories

- Application controls are commonly grouped into five categories

Type	Description	Examples
Edit Checks	Limit risk of inappropriate input, processing or output of data due to field format.	► Required fields
Validations	Limit risk of inappropriate input, processing, or output of data due to the confirmation of a condition.	► 3-way match ► Tolerance limits
Calculations	Ensure that a computation is occurring accurately	► Accounts receivable aging ► Pricing calculations
Interfaces	Limit risk of inappropriate input, processing, or output of data being exchanged from one application to another	► Duplicate record checks ► Error reporting during batch runs
Authorizations	Limit the risk of inappropriate input, processing, or output of key financial data due to unauthorized access to key financial functions or data; includes: ► Segregation of incompatible duties ► Authorization checks, limits and hierarchies.	► Approval to post journal entries

Embedded Application Controls

- An **Embedded** control is programmed within application logic and can be modified only through code changes
  - Such changes are subject to change management controls
  - As a result, the following should be performed for embedded controls:
    - Obtain evidence and document on the leadsheet that the control is embedded and not configurable
      - Sources may include user manual, training material or other documentation
      - If documentation does not exist, then inquiry is sufficient and documentation should include the name(s) of the person inquired of
    - Perform a walkthrough/test of one of the control including both positive and negative test scenarios

Configurable Application Controls

- A **configurable** control functions according to key application settings that can be modified by certain users
  - Such changes are not typically subject to change management controls and should be tested as follows:
    - Obtain evidence and document that the control is configurable and the system is properly configured to support execution of the control (e.g., screen prints of the configuration)
    - Obtain system-generated evidence of users who have access to modify the setting and validate for appropriateness
    - Where possible, obtain evidence showing the last time the configurable setting was modified
    - Perform a walkthrough/test of one of the control including both positive and negative test scenarios

Other application control testing considerations

- Test all potential outcomes/scenarios of the application control, including both positive and negative testing procedures.
- **Inquire and document** whether an override of the application control is possible. When overrides are possible, we consider how management monitors transactions that bypass the control.
- Perform application control testing in the production environment when possible. If this is not possible, we consider and **document** whether the non-production environment closely resembles production.
- When using the “test of one” approach strategy for application controls across multiple in-scope locations, we should **document** the sufficiency of evidence on how we confirmed consistency of the information systems across locations (ITGCs).

Questions?