Controls Fundamentals

Internal Control Concepts & Strategies
CJ Higgins
Manager
Risk Advisory & Consulting Practice
You will be able to:

- Understand why we need controls
- Identify Entity Level Controls ("ELCs")
- Identify IT General Controls ("ITGCs")
- Identify control types
  - Manual Controls
  - IT Dependent Manual Controls ("ITDM")
  - Application Controls
- Understand Preventative vs Detective Controls
- Understand IPE/IUC
- Understand your role as a "Control Owner"
Budding Opportunity for Internal Controls

- Internal control are the mechanisms, rules, and procedures implemented by a company to ensure the integrity of financial information, promote accountability, and prevent fraud.

- Management has prioritized a commitment to effective internal controls to support growth and successfully manage the increasing complexity of operations and accelerating pace of change.

- Management will help consider the following activities and bring to life a robust, value-add control environment:
  - Workflow routing
  - Calculations
  - Interfaces
  - Master data management and security
  - Approval thresholds
  - Audit logging
  - BoD Considerations
  - Account reconciliations
  - Evidence retention
  - Policies & Procedures
  - Intelligent user role design / SOD
  - Templates
  - Key report baseline
Benefits of Implementing Internal Controls

• Reduce financial misstatements and errors
• Increase credibility with stakeholders
• Apply correct and consistent accounting treatment with confidence, discipline, and consistency
• Support well-managed growth
• Improve employee knowledge
• Clear roles and responsibilities
• Enhance accountability and trust
The Controls Environment

Entity Level Controls

Financial Reporting

Business Process Controls

Automated Controls

IT Dependent Controls

SOD/Operations

Access Security

Change Management

All rights reserved. Frazier & Deeter, 2021.
# Types of Controls

Controls are typically divided into the following categories:

<table>
<thead>
<tr>
<th>Control Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity-Level Controls (ELCs)</td>
<td>Controls throughout the organization to mitigate risks threatening the organization as a whole and to provide assurance that organizational objectives are achieved.</td>
</tr>
<tr>
<td>IT General Controls</td>
<td>Controls related to IT environment – infrastructure, applications, databases, operating systems, etc. (user security, program change management, backups, passwords, incident management, maintenance, etc.)</td>
</tr>
<tr>
<td>Manual</td>
<td>Activity performed without reliance or influence on technology (observation, manual control signing, etc.)</td>
</tr>
<tr>
<td>IT-Dependent Manual</td>
<td>Controls that involve IT generated reports or other IT functionality combined with human procedures (report review, workflow approval, reconciliations, etc.)</td>
</tr>
<tr>
<td>Application</td>
<td>Embedded in applications; configurations; resides in logic / core functionality; cannot be circumvented; (rules, calculations, transaction mapping, data flow routing, interface, exception reports, etc.)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nature of Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive</td>
<td>Control avoids exception / unexpected condition before it occurs or prevents it from happening (edit check, workflow approval, etc.)</td>
</tr>
<tr>
<td>Detective</td>
<td>Control identifies exception / unexpected condition after completing the control activity (reconciliation, variance analysis, audit, etc.)</td>
</tr>
</tbody>
</table>
Entity Level Controls
Entity Level Controls

- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring
- Controls Environment
Entity Level Controls

Controls Environment
- Commitments to Integrity
- BOD Independence
- Retain and attract talent
- Accountability for controls

Risk Assessment
- Setting objectives
- Identifying risks
- Fraud risk assessments
- Assessing external and internal changes

Control Activities
- Risk-based control assessment
- ITGC framework
- Company policy and procedure documentation

All rights reserved. Frazier & Deeter, 2021.
Entity Level Controls

Information & Communication
- Processing of information
- Internal communication
- External communication

Monitoring
- Evaluation of internal control
- Communication of control deficiencies
- Remediation of control deficiencies
IT General Controls
Numerous information systems are used to process and record transactions and data that affect financial reporting.

Configurations, rulesets, workflows, interfaces, etc. represent critical elements of the Company’s overall control environment.

IT general controls ("ITGCs") related to access provisioning, change management and IT operations must be effective to fully rely on the IT systems.

ITGCs enable reliance on system generated reports, application controls, and transaction processing.
## More About IT General Controls

<table>
<thead>
<tr>
<th>IT Process Area</th>
<th>Control Guide</th>
</tr>
</thead>
</table>
| **1. User provisioning** | - User provisioning – new users  
                          - User provisioning – modified access  
                          - User provisioning – terminated users  
                          - User provisioning – contractors  
                          - Privileged access is restricted  
                          - Role-based access reviews |
| **2. Change management** | - Changes are documented and approved  
                          - Changes are tested prior to go-live  
                          - Developer access to production is prohibited  
                          - Separate environments are maintained (dev/test/QA/prod) |
| **3. IT Operations** | - Job scheduling / processing  
                          - Backups and restoration  
                          - Physical security  
                          - Data center  
                          - Incident management |
| **4. Security** | - Passwords  
                          - Firewall configurations  
                          - Remote access  
                          - Policies and Methodologies  
                          - Vendor Management and Oversight  
                          - Tools |
| **5. Governance** | - Policies and Methodologies  
                          - Steering Committee(s)  
                          - Vendor Management and Oversight  
                          - Tools |
Manual Controls
Manual Controls

- Controls performed by individuals
- Not reliant on IT generated reports for the underlying information
- Example: Daily, cash received via Lockbox is reconciled to the wholesale sales receipts by Accounting. All variances are investigated
IT Dependent Manual Controls
ITDM Controls

- Control manually performed by an individual
- Relies on system-generated information to perform the control
- Majority of controls performed by management
Examples of ITDM Controls

- Employee reimbursements reviewed and approved prior to disbursement
- New customers are reviewed and approved before being added to the system
- Inventory obsolescence reserve calculation is reviewed and approved by a member in Operations and Finance
- Timesheets are reviewed and approved by the employee's supervisor before payroll is processed to ensure timesheet are accurate
Application Controls

- Application controls are highly important and highly efficient.
- Applies to business rules intended to be enforced automatically/systematically (i.e. input, processing, and output controls).
- Key to a) identify and document during design phase of a large system implementation project and b) test prior to go-live.

<table>
<thead>
<tr>
<th>Input</th>
<th>Processing</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure complete and accurate recording of authorized transactions by only authorized users</td>
<td>Ensure complete and accurate processing of authorized transactions</td>
<td>Ensure that a complete and accurate data set is posted/reported</td>
</tr>
<tr>
<td>Apply rules to accept, reject, suspend entries</td>
<td>Batch totals</td>
<td>Changes reports</td>
</tr>
<tr>
<td>Prevents unwanted duplications</td>
<td>Audit trails</td>
<td>Distribution registers</td>
</tr>
<tr>
<td></td>
<td>Cut-off assurance</td>
<td>Error listings</td>
</tr>
</tbody>
</table>
Application Control Examples

▪ The ERP system reduces inventory and records cost of goods sold upon sale
▪ The ERP system prevents duplicate journal entry numbers
▪ The system Prevents Duplicate Invoices
▪ The system prevents sales orders to be processed when the open sales orders exceed the customer's credit limit or if the customer is placed on a "do not ship" restriction
▪ Depreciation is calculated monthly by F&O
Preventative vs Detective Controls
Preventative vs Detective Controls

**Preventative**
- Designed to keep errors or irregularities from occurring
- Heavy on initiation and application controls
- Emphasis on preventive measures, such as proper user access and segregation of duties

**Detective**
- Designed to detect errors
- Want to identify what occurred, how did it occur, and what can be implemented to prevent from happening
- Think Management Review Controls
Preventative vs Detective Control Examples

**Preventative**
- Inventory is safeguarded in a secure, limited access facility. Only authorized individuals can access the inventory.
- Each ERP system user has a unique ID.
- New vendors are reviewed and approved before being added to the system.
- All cash disbursements require 2 approvals verifying the amount and authorizing the disbursement.

**Detective**
- Management reviews the accuracy and completeness of all ROU accounts through account reconciliations.
- On a quarterly basis, the Controller reviews and approves the variance report.
- AP Accruals are reviewed and approved.
- Daily, cash received via Lockbox is reconciled to the wholesale sales receipts by Accounting. All variances are investigated.
What is IPE/IUC?

- IPE – Information Produced by the Entity
- IUC – Information Used in a Control
- In short, IPE/IUC is any document which is relied upon to perform assurance procedures
- Not just reports – any “information” produced by the entity
- Heavy emphasis by auditors to ensure completeness and accuracy of information
What does IPE apply to?

IPE/IUC applies to

- Accumulations (such as reports, schedules, lists, data files or analyses) of:
  - Financial information
  - Non-financial information used to determine financial transactions created by the entity or service organization
  - Manually prepared documents being used as audit evidence
What to look for when receiving IPE/IUC for a population?

- Key areas to look for to validate Completeness & Accuracy (C&A):

  1. Query/Parameters used to generate report - to determine all necessary fields are included, and if any fields were excluded that would impact the output/population.

  2. Sample data in the resulting report/output
     - Trace details to the output based on details confirmed with the process owner
     - Document Row/Page Count from the report to determine the total output from a system matches output obtained.
     - Document the date a report was generated

  3. Identify data sources (e.g. application, database, report generation tool)
What Can Go Wrong with IPE/IUC?

▪ What are the potential risks of not properly understanding and documenting IPE/IUC?
  ▪ Not all data may be captured as originally expected
  ▪ Report logic may be incorrect
  ▪ Spreadsheet sorting errors can exist or contain hidden formulas
  ▪ Report parameters may have been entered incorrectly
  ▪ Inappropriate or unauthorized changes are made to reports unknowingly
  ▪ Issues may not be identified such as input errors, incorrect source data

▪ What are some ways to address the risks of bad IPE/IUC?
  ▪ Apply Audit procedures over the IPE addressing source of the information, report logic, and parameters used for generation
  ▪ Testing controls over the creation of IPE
  ▪ Substantively testing IPE
  ▪ Using a combination of tests of controls and substantive testing
Control Owner Responsibilities
Becoming a Control Owner

• You received a call to talk about your role at the Company
• A few weeks later, you receive an email that you are now the “Control Owner” for a control
• What does it mean to be a “Control Owner”?
Control Owner Responsibilities

- Know the controls you are responsible to deliver and confirm that the control documentation is accurate
- Take ownership for defining and describing objective of the control and related steps
- Identify and communicate opportunities for improved efficiency or effectiveness
- Anticipate and communicate any changes in the business and processes or tools
- Understand source of data used in performance of control and/or recording of transactions
- Execute performance of control and maintain documentation evidencing the control occurred
- Respond timely to the auditors for any process or testing questions
Control Testing Outcomes

Control Passes
Both the design and operation of the control mitigate the risk identified.

Control Deficiency
A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

- A deficiency in *design* exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met.

- A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or competence to perform the control effectively.
Control Testing Outcomes

**Significant Deficiency ("SD")**

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting.

**Material Weakness ("MW")**

A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.
Control Examples
Control Example

Control

Account reconciliations are performed monthly then reviewed and approved by an individual at least one level than the preparer within 30 days.

Attributes of the control

A) The account reconciliation is prepared timely
B) Supporting evidence is retained to support the performance of the reconciliation
C) The account reconciliation is reviewed timely and appropriately
D) Precision of review is adequate to support the reconciliation
E) Appropriate IPE is retained to ensure completeness and accuracy of the information used in the reconciliation
Passing Control Example

Control

Account reconciliations are performed monthly then reviewed and approved by an individual at least one level than the preparer within 30 days.

Evidence to support the operating effectiveness of the control

- Evidence of preparation is retained, including evidence of who performed and date
- Supporting documentation (including IPE) is retained with the reconciliation
- Supporting documentation agrees to the values per the reconciliation
- Evidence of review is retained, including who reviewed and date
- Appropriate IPE is retained for all supporting documentation
Remote Work Considerations
Additional Considerations

With the impact of COVID and increased reliance on remote work, a variety of risks have been increased and/or impacted significantly:

- Data security – Reliance on IT and security awareness
- Changes in control processes/procedures – Communication is key
- Increased reliance on IPE
- Changes in staffing – Are you able to maintain proper SoD?
- Manually performed processes no longer performed – What is in place?
- Increased reliance on IT
Questions