COSO Updates and Expectations

IIA – San Diego Chapter
January 8, 2014
Agenda

• Overview of 2013 Internal Control-Integrated Framework and Companion Guidance
• 2013 Framework General Enhancements by Component
• Transition
• Considerations and Next Steps
• Internal Control Hot Topics
• Appendix A
  • Risk Assessment (principles 7, 8, 9)
  • Information & Communication (principle 13)
  • Outsourced Service Providers (principles 10, 16)
## 2013 Framework and Guidance

<table>
<thead>
<tr>
<th>Components</th>
<th>Summarized Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Environment</strong></td>
<td>1. Demonstrates commitment to integrity and ethical values</td>
</tr>
<tr>
<td></td>
<td>2. Exercises oversight responsibility</td>
</tr>
<tr>
<td></td>
<td>3. Establishes structure, authority and responsibility</td>
</tr>
<tr>
<td></td>
<td>4. Demonstrates commitment to competence</td>
</tr>
<tr>
<td></td>
<td>5. Enforces accountability</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>6. Specifies relevant objectives</td>
</tr>
<tr>
<td></td>
<td>7. Identifies and analyzes risk</td>
</tr>
<tr>
<td></td>
<td>8. Assesses fraud risk</td>
</tr>
<tr>
<td></td>
<td>9. Identifies and analyzes significant change</td>
</tr>
<tr>
<td><strong>Control Activities</strong></td>
<td>10. Selects and develops control activities</td>
</tr>
<tr>
<td></td>
<td>11. Selects and develops general controls over technology</td>
</tr>
<tr>
<td></td>
<td>12. Deploys through policies and procedures</td>
</tr>
<tr>
<td><strong>Information &amp; Communication</strong></td>
<td>13. Uses relevant information</td>
</tr>
<tr>
<td></td>
<td>14. Communicates internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicates externally</td>
</tr>
<tr>
<td><strong>Monitoring Activities</strong></td>
<td>16. Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates deficiencies</td>
</tr>
</tbody>
</table>
2013 Framework and Guidance (cont.)

Specific significant enhancements to the 1992 Framework that may pose challenges to management:

Risk Assessment

- More detailed discussions about risk assessment concepts, including those related to inherent risk, risk tolerance, how risks may be managed, and linkage between risk assessment and control activities
- Considering the potential for fraud risk when assessing risks to the achievement of an organization’s objectives

Outsourcing Service Providers (OSPs)

- Considerations related to OSPs are included throughout the framework, including 12 out of 17 principles
- Requires management to specifically consider how OSP’s are monitored

Information Technology (IT)

- Considerations related to IT are included in 14 of 17 principles
- Discussion of using IT to assist in continuous monitoring
- Requirements for ensuring quality of information (data integrity)
# 2013 Framework and Guidance

## Control Environment

### Use of principles to describe components

<table>
<thead>
<tr>
<th>Component</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control environment</td>
<td>1. Demonstrates commitment to integrity and ethical values</td>
</tr>
<tr>
<td></td>
<td>2. Board demonstrates independence and exercises oversight</td>
</tr>
<tr>
<td></td>
<td>3. Management establishes structure, authority, and responsibility</td>
</tr>
<tr>
<td></td>
<td>4. Organization demonstrates commitment to competence</td>
</tr>
<tr>
<td></td>
<td>5. Enforces accountability</td>
</tr>
</tbody>
</table>

### Enhancements Include

- Setting expectations for standards of conduct (with employees and outsourced service providers), evaluating adherence to such standards, and addressing deviations in a timely manner
- Matters related to board independence, skills and expertise
- Importance of accountability for internal control
- Planning and preparing for succession for those roles important to the effectiveness of internal control
- Aligning incentives and rewards with internal control responsibilities
## 2013 Framework and Guidance (cont.)

### Use of principles to describe components

<table>
<thead>
<tr>
<th>Component</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>6. Specifies relevant objectives</td>
</tr>
<tr>
<td></td>
<td>7. Identifies and analyzes risk</td>
</tr>
<tr>
<td></td>
<td>8. Assesses fraud risk</td>
</tr>
<tr>
<td></td>
<td>9. Identifies and analyzes significant change</td>
</tr>
</tbody>
</table>

### Enhancements Include

- Explains that the risk assessment process includes risk identification, analysis, and response
- Considers velocity and persistence of risk (in addition to impact and likelihood)
- Includes fraud risk assessment as a principle
- Incorporates considerations of outsourced service providers
- Importance of evaluating changes in the external environment, business model, operations, technology, relationships with outsourced service providers, leadership and how such changes impact internal control
## Use of principles to describe components

<table>
<thead>
<tr>
<th>Component</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control activities</td>
<td>10. Selects and develops control activities</td>
</tr>
<tr>
<td></td>
<td>11. Selects and develops general controls over technology</td>
</tr>
<tr>
<td></td>
<td>12. Deploys through policies and procedures</td>
</tr>
</tbody>
</table>

**Enhancements Include**

- Emphasis on the linkage between risk assessment and control activities
- The types of control activities applied (including considering preventative vs. detective controls)
- Incorporates updated technology concepts, including those related to technology infrastructure, security, acquisition, development, maintenance, and use of OSPs
- Establishing responsibility and accountability for executing policies and procedures
- Reassessing policies and procedures on a periodic basis to determine their continued relevance and if revisions are needed
### Use of principles to describe components

<table>
<thead>
<tr>
<th>Component</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information and communication</td>
<td>13. Uses relevant and quality information</td>
</tr>
<tr>
<td></td>
<td>14. Communicates internally</td>
</tr>
<tr>
<td></td>
<td>15. Communicates externally</td>
</tr>
</tbody>
</table>

**Enhancements Include**

- Identifying information requirements, verifying sources of data, processing relevant data, maintaining quality through processing, and using OSPs
- Considering reliability and protection of data
- Reevaluating information needs
- Considering how information supports the functioning of internal control
- Providing separate channels of communication for anonymous or confidential communication when normal communication channels are inoperative or ineffective (e.g., through whistle-blower hotlines)
### Use of principles to describe components

<table>
<thead>
<tr>
<th>Component</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring activities</td>
<td>16. Conducts ongoing and/or separate evaluations</td>
</tr>
<tr>
<td></td>
<td>17. Evaluates and communicates deficiencies</td>
</tr>
</tbody>
</table>

**Enhancements Include**

- Considerations of the rate of change when developing monitoring activities
- Using a baseline of understanding to establish plans for ongoing and separate evaluations
- Considerations related to monitoring at different levels of an organization and monitoring of OSPs
- Using technology in the context of monitoring
- Communicating deficiencies
- Monitoring corrective actions
2013 Framework
Effective system of internal control

• Per COSO, an effective system of internal control requires:
  – Each of the five components of internal control and relevant principles are present and functioning
  – The five components are operating together in an integrated manner

• If a major deficiency (or material weakness) exists, cannot conclude that the system of internal control is effective
  – For purposes of complying with requirements of the Sarbanes-Oxley Act of 2002, internal control deficiency classification criteria established by the SEC and PCAOB must be used.
Illustrative Tools
What are they?

• Intended to assist entities when assessing effectiveness of internal control
  – The Illustrative Tools can help management assess whether:
    • Each of the five components and relevant principles are present and functioning
    • The five components are operating together in an integrated manner

• Organized in three sections:
  – Introduction
  – Templates
  – Scenarios
ICEFR Compendium
What is it?

• Illustrates how entities can apply the 2013 Framework to design, implement, and conduct a system of ICEFR

• Provides examples and approaches for applying the 17 principles
  – **Approaches** describe how organizations may apply the principles within their system of ICEFR
  – **Examples** provide specific illustrations to users on the application of each principle
Transition

COSO transition guidance

• 2013 Internal Control-Integrated Framework (the “2013 Framework”) and illustrative documents issued:
  May 14, 2013

• Transition period as announced by COSO:
  – COSO will consider the 1992 Framework superseded after December 15, 2014

• If applying and referencing COSO’s Internal Control–Integrated Framework for external reporting purposes:
  – Annual external reporting should clearly disclose whether the 1992 or 2013 Framework was utilized
Considerations and Next Steps
Considerations and Next Steps

Understand and Educate

- Read 2013 Framework
- Identify new concepts and changes
- Consider training and education needs

Assess

- Assess and evaluate needs regarding control objectives for operations, compliance, and non-financial reporting
- Determine impacts on the entity’s design and evaluation of ICFR
  - Assess coverage of the principles and consider points of focus
  - Assess current processes, activities, and available documentation regarding meeting the principles
  - Identify any gaps

Plan and Implement

- Identify the steps that need to be performed to transition to the 2013 Framework
- Formulate a plan to transition by December 15, 2014
- Take appropriate steps to implement plan

Communicate

- Communicate internally with all groups responsible for implementing, monitoring, and reporting on the organization’s internal control
- Discuss and coordinate activities with internal audit (if applicable) and the external auditor
Opportunities for Companies

• Implementation of the 2013 Framework provides a good opportunity to create value for organizations and refresh internal control systems, regardless of maturity level of an internal control system.
  – Synergies and simplifications may be available
  – May also identify gaps in design and operating effectiveness to be addressed
    • E.g., fraud risk assessment programs, IT controls, and monitoring of outsourced service providers
  – May also identify gaps in documentation and evidentiary support for evaluating the effectiveness of internal control under the 2013 Framework
  – Opportunities to improve operations, compliance, and reporting
Internal Control Hot Topics
### 2013 Framework and Guidance

**Hot Topics and Areas of Focus for Management**

<table>
<thead>
<tr>
<th></th>
<th>Risk assessment process to identify:</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>• The likely sources of misstatement (supported by sufficiently detailed process descriptions/flow diagrams)</td>
<td>7, 9, and 12</td>
</tr>
<tr>
<td></td>
<td>• The relevant controls (documented in sufficient detail to communicate expectations, enable effective monitoring)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Significant changes that result in new risks that require new or modified controls</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Fraud risk assessment, including audit committee oversight of risk of management override</td>
<td>Principle 8</td>
</tr>
<tr>
<td>3</td>
<td>Effectiveness of control environment</td>
<td>Principles 1-5</td>
</tr>
<tr>
<td></td>
<td>• The entity’s commitment to integrity and ethical values</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The audit committee</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Appropriateness of segregation of duties</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Controls over outsourced service providers and specialists</td>
<td>Throughout</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>5</td>
<td>Precision of management review controls, including mitigation of bias in the decision-making</td>
<td>Principle 10</td>
</tr>
<tr>
<td>6</td>
<td>Controls over accuracy and completeness of reports or data: • Produced by the entity, both system and non-system generated reports (e.g. excel spreadsheets) • From service organizations • From third parties</td>
<td>Principle 13</td>
</tr>
<tr>
<td>7</td>
<td>Controls over: • One-time transactions, significant unusual transactions • Disclosures • Cash flow statement</td>
<td>Principles 10 and 12</td>
</tr>
</tbody>
</table>
# 2013 Framework and Guidance

## Hot Topics and Areas of Focus for Management

<table>
<thead>
<tr>
<th>Principle</th>
<th>Information Technology Controls:</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Linkage of financial reporting data, automated controls and IPE to relevant IT applications and infrastructure</td>
</tr>
<tr>
<td></td>
<td>Consideration of IT risks related to interfaces, data warehouses, and third parties</td>
</tr>
<tr>
<td></td>
<td>Concluding IT risks and their effect on financial reporting</td>
</tr>
<tr>
<td>Principle</td>
<td>Deficiencies:</td>
</tr>
<tr>
<td>9</td>
<td>Basis for concluding on severity, including consideration of root causes</td>
</tr>
<tr>
<td></td>
<td>Aggregation of deficiencies</td>
</tr>
<tr>
<td></td>
<td>Effectiveness of remediation process</td>
</tr>
<tr>
<td></td>
<td>Concluding on IT deficiencies</td>
</tr>
<tr>
<td>Principle</td>
<td>Monitoring activities:</td>
</tr>
<tr>
<td>10</td>
<td>Alignment with the detailed risk assessment</td>
</tr>
<tr>
<td></td>
<td>Obtaining persuasive evidence of effectiveness, not just occurrence</td>
</tr>
<tr>
<td></td>
<td>Approach to insignificant components, particularly in emerging markets</td>
</tr>
</tbody>
</table>
Top 10 Internal Control Issues

Top 10 Internal Control Adverse Opinions

- Accounting Personnel / Competence / Training
- Segregation of Duties
- Material / Numerous YE Adjustments
- Ineffective / Understaffed Audit Committee
- Inadequate Disclosure Controls
- Non-routine Transaction Control Issues
- IT Software, Security, Access Issue
- Untimely or Inadequate Account Reconciliations
- Restatement / Non-reliance of Company Filings
- Insufficient Non-Existent IA Function

Source: Audit Analytics – SOX 404 Dashboard
Resources:

- Deloitte Heads Up
  - [www.Deloitte.com](http://www.Deloitte.com)

- New guidance available for purchase through link on COSO website:
  - [www.coso.org](http://www.coso.org)

Contact Info:

- Cecile Galvez
  - cegalvez@deloitte.com
  - 619-237-6870

- John Giakouminakis
  - jgiakouminakis@deloitte.com
  - 213-688-3384
Appendix A

Focus on:
Risk Assessment (7, 8, 9)
Information & Communication (13)
Outsourced Service Providers (10, 16)
Risk Assessment Principle 7
Identifies, Analyzes and Responds to Risk

“The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed”

- Identifying and analyzing risks is an ongoing iterative process
- Management considers risks at all levels of the entity and takes the necessary actions to respond

<table>
<thead>
<tr>
<th>Points of Focus</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Includes entity, subsidiary, division, operating unit, and functional levels</td>
<td>Identify</td>
</tr>
<tr>
<td>• Analyzes internal and external factors</td>
<td>Analyze</td>
</tr>
<tr>
<td>• Involves appropriate levels of management</td>
<td></td>
</tr>
<tr>
<td>• Estimates significance of risks identified</td>
<td></td>
</tr>
<tr>
<td>• Determines how to respond to risk</td>
<td>Respond</td>
</tr>
</tbody>
</table>
## Risk Assessment Principle 7
Identifies, Analyzes and Responds to Risk

<table>
<thead>
<tr>
<th>Enhanced Aspects of Principle 7:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Details that risk assessment includes identification, analysis, and response.</td>
</tr>
<tr>
<td>• Incorporates the concepts of inherent risk.</td>
</tr>
<tr>
<td>• Expands discussion regarding risk tolerance and how risk may be managed, including through acceptance, avoidance, reducing, and sharing risk.</td>
</tr>
<tr>
<td>• Considers velocity and persistence of risk (in addition to impact and likelihood).</td>
</tr>
<tr>
<td>• Incorporates consideration of outsourced service providers.</td>
</tr>
</tbody>
</table>
### ICEFR Compendium

#### Principle 7: Identifies, Analyzes, Responds to Risk

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Applying a Risk Identification Process</td>
<td>• Analyzing Risk Across Functions</td>
</tr>
<tr>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
</tr>
<tr>
<td>• Meeting with Entity Personnel</td>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
</tr>
<tr>
<td>• Assessing the Likelihood and Significance of Identified Risks</td>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
</tr>
<tr>
<td>• Considering Internal and External Factors</td>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
</tr>
<tr>
<td>• Evaluating Risk Responses</td>
<td>• Assessing Risks to Significant Financial Statement Accounts</td>
</tr>
<tr>
<td></td>
<td>• Using Risk Ratings</td>
</tr>
<tr>
<td></td>
<td>• Analyzing Risk for Information Technology</td>
</tr>
<tr>
<td></td>
<td>• Identifying and Responding to Risk</td>
</tr>
<tr>
<td></td>
<td>• Using Benchmark Data to Assess Significance and Response to Risk</td>
</tr>
<tr>
<td></td>
<td>• Analyzing Risks from External Factors</td>
</tr>
<tr>
<td></td>
<td>• Considering Changes in Information Systems</td>
</tr>
<tr>
<td></td>
<td>• Considering Risk Response in a Revenue Process</td>
</tr>
</tbody>
</table>
ICEFR Compendium

Example: Analyzing Risk Across Functions

• The CFO holds a working session of department leaders from marketing, production, IT, HR, and administration to perform a risk analysis by department.

• Risks are rated from 1 (least risk) to 5 (most risk) based on potential impact on financial reporting and likelihood of occurrence.

• After the discussion sessions, the participants document the results in a table that outlines each specific risk together with the rating and factors contributing to the rating.

• For example, revenue recognition was rated as 4 (medium-high). Contributing to this assessment was consideration of the likelihood and impact of the organization failing to:
  • Transfer ownership on specific sales in accordance with revenue recognition accounting standards for goods sold on consignment.
  • Account for complex sales promotions and discounts completely and accurately
  • Update IT systems to account for complex revenue transactions that could lead to inappropriate recognition of revenue
Risk Assessment Principle 8
Assesses Fraud Risk

“The organization considers the potential for fraud in assessing risks to the achievement of objectives”

Points of Focus:

• Considers various types of fraud
• Assesses incentive and pressures
• Assesses opportunities
• Assesses attitudes and rationalization

Enhanced Aspects of Principle 8:

• Incorporates the concept of fraud risk assessment.

• Considerations related to various types of fraud, including fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets, management override, safeguarding of assets, and corruption.

• Evaluating incentives and pressures, opportunities, and attitudes and rationalizations.

• Incorporates considerations related to outsourced service providers.
As part of the risk assessment process, organizations should *identify the various ways that fraudulent financial reporting can occur*, considering:

<table>
<thead>
<tr>
<th>Risk Assessment Principle 8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assesses Fraud Risk</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- Management bias, for instance in selecting accounting principles
- Degree of estimates and judgments in external reporting
- Fraud schemes and scenarios common to the industry sectors and markets in which the entity operates
- Geographic regions where the entity does business
- Incentives that may motivate fraudulent behavior
- Nature of technology and management’s ability to manipulate information
- Unusual or complex transactions subject to significant management influence
- Vulnerability to management override and potential schemes to circumvent existing control activities
ICEFR Compendium
Principle 8: Assesses Fraud Risk

ICEFR Approaches

• Conducting Fraud Risk Assessments
• Considering Approaches to Circumvent or Override Controls
• Considering Fraud Risk in the Internal Audit Plan
• Reviewing Incentives and Pressures Related to Compensation Programs

ICEFR Examples

• Assessing Fraud Risk
• Maintaining Oversight
• Identifying and Analyzing Risk of Material Omission and Misstatement Due to Fraud
• Analyzing Compensation Structure

Additional Resources:
• Management Override of Internal Controls: The Achilles’ Heel of Fraud Prevention
• Management Antifraud Programs and Controls: Guidance to Help Prevent, Deter, and Detect Fraud
ICEFR Compendium
Example: Assessing Fraud Risk

The chief compliance officer at a global retail operation, annually conducts a fraud risk assessment. In doing so, he interviews management at all the international locations about fraud issues. He analyzes:

- Historical fraud, including theft of inventory and the processes in place to identify and record such theft
- The methodology used for recording and calculating inventory and shrinkage
- Whistle-blower reports
- The number of manual entries vs. automated entries recorded
- The number of late entries due to subjective estimates

With this information, the chief compliance officer:

- Forms a preliminary view of the potential fraud activities, which he discusses with management of each jurisdiction in order to consider implications and what control activities can reduce the risk of fraud.
- Has discussions with human resources personnel and reviews information in the staff files.
- Uses his historical knowledge and staff information to assess the attitude of the local management toward the tolerance of fraud and to determine whether local management may rationalize fraudulent activities, including corruption.
- Once complete, submits a report to the audit committee for its consideration.
ICEFR Compendium

Example: Maintaining Oversight

The audit committee of a medical supply company takes the issue of management override of controls very seriously. Consequently, every quarter the committee reviews the fraud risk assessment process. In doing so, the members of the audit committee:

• Maintain an appropriate level of skepticism
• Discuss management’s assessment of fraud risks
• Use the code of conduct to assess financial reporting culture
• Ensure the entity has a robust whistle-blower program
• Develop a broad information and feedback network

In addition, the audit committee asks the chief audit executive about:

• What fraud risks are being monitored by the internal audit team on a periodic or regular basis
• What specific procedures internal audit performs to address management override of internal controls
• Whether anything has occurred that would lead internal audit to change its assessment of the risk of management override of internal controls.

With this information in hand, the audit committee discusses with the full board and senior management any concerns that need added management focus.
Challenge Your Fraud Risk Assessment

Instances of Material Frauds

- Revenue recognition: 38%
- Improper disclosures: 12%
- Manipulation of expense: 12%
- Manipulation of liabilities: 8%
- Manipulation of assets: 7%
- Manipulation of reserves: 7%
- Bribery and kickbacks: 4%
- Asset misappropriation: 3%
- Manipulation of A/R: 3%
- Investments: 2%
- Goodwill: 2%
- Aiding and abetting: 2%

Source: Deloitte Forensic Center
Risk Assessment Principle 9
Identifies and Analyzes Significant Changes

“The organization identifies and assesses changes that could significantly impact the system of internal control”

Points of Focus

• Assesses changes in the external environment
• Assesses changes in the business model
• Assesses changes in leadership

Enhanced Aspects of Principle 9

• Importance of assessing changes in the external environment, business model, operations, technology, and leadership and how such changes may impact internal control.
# ICEFR Compendium

**Principle 9: Identifies and Analyzes Significant Changes**

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assessing Change in the External Environment</td>
<td>• Reacting to Significant Change Caused by External Factors</td>
</tr>
<tr>
<td>• Conducting Risk Assessments Relating to Significant Change</td>
<td>• Updating Risk Assessments For a New CEO</td>
</tr>
<tr>
<td>• Considering Change through Succession</td>
<td>• Responding to Significant Change Due to International Exposure</td>
</tr>
<tr>
<td>• Considering CEO and Senior Executive Changes</td>
<td>• Responding to Significant Change from an Acquisition</td>
</tr>
<tr>
<td></td>
<td>• Planning for Executive Transition</td>
</tr>
<tr>
<td></td>
<td>• Preparing for a Change in CEO</td>
</tr>
</tbody>
</table>
ICEFR Compendium

Example: Responding to Significant Change Due to International Exposure

Consecutive Corp., a multi-billion-dollar technology equipment manufacturer that has historically focused on sales in the United States, has decided to expand internationally with both sales and manufacturing. As part of the expansion plans, Consecutive has assessed several factors:

- Incremental revenue opportunities
- Competition in the marketplace
- Cultural dynamics of the targeted international location
- Different laws and regulations, including those that would affect the company’s ability to defend its patents
- Risk of increased fraud from theft and corruption

Each of these factors presents incremental risks to financial reporting and processes that need to be managed. Therefore, Consecutive’s corporate controller is performing a risk assessment with the finance teams in the international locations to ensure these new risks are identified and to help management determine how best to respond.
Information & Communication Principle 13

Uses Relevant Information

“The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.”

Points of Focus

• Identifies information requirements
• Captures internal and external sources of data
• Processes relevant data into information
• Maintains quality throughout processing
• Considers costs and benefits

Enhanced Aspects of Principle 13

• Identifying information requirements, processing relevant data, maintaining quality through processing
• Verifying the sources of data and considering the reliability and protection of data
• Considering the costs and benefits of information, impact of technology, and use of outsourced service providers
• Considering how information supports the functioning of internal control.
• Reevaluating information needs
## ICEFR Compendium

### Principle 13: Uses Relevant Information

<table>
<thead>
<tr>
<th><strong>ICEFR Approaches</strong></th>
<th><strong>ICEFR Examples</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creating an Inventory of Information Requirements</td>
<td>• Evaluating Business Activities to Identify Information Requirements</td>
</tr>
<tr>
<td>• Obtaining Information from External Sources</td>
<td>• Maintaining Data Flow Diagrams, Flowcharts, Narratives, and Procedures Manuals</td>
</tr>
<tr>
<td>• Obtaining Information from Non-Finance Management</td>
<td>• Gathering Information from External Sources</td>
</tr>
<tr>
<td>• Creating and Maintaining Information Repositories</td>
<td>• Capturing Information through Electronic Data Interchange</td>
</tr>
<tr>
<td></td>
<td>• Conducting Quarterly Interviews of Operations and Other Management</td>
</tr>
<tr>
<td></td>
<td>• Obtaining Operating Information for Financial Reporting</td>
</tr>
<tr>
<td></td>
<td>• Using a Data Warehouse to Facilitate Access to Information</td>
</tr>
</tbody>
</table>
ICEFR Compendium

Principle 13: Uses Relevant Information

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Using an Application to Process Data into Information</td>
<td>• Data Capture and Processing for the Purchasing and Payables Cycle</td>
</tr>
<tr>
<td>• Enhancing Information Quality through a Data Governance Program</td>
<td>• Validating Data and Information</td>
</tr>
<tr>
<td>• Identifying, Securing, and Retaining Financial Data and Information</td>
<td>• Identifying and Protecting Financial Data and Information</td>
</tr>
<tr>
<td></td>
<td>• Identifying and Classifying Data for Financial Reporting</td>
</tr>
</tbody>
</table>
ICEFR Compendium

Example: Using a Data Warehouse to Facilitate Access to Information

• A food distributor has recently completed an enterprise-reporting project to identify and inventory information used across the company for external financial reporting and related internal control. The results of the project were used by the chief information officer and chief financial officer to design a company-wide data warehouse and reporting tools that would support a single source for financially relevant information.

• The first phase of the project involved creating an inventory of the existing reports identifying relevant sources and eliminating non-critical and redundant reports.

• The second phase involved designing and implementing the functional and technical capabilities needed to capture and store data used to generate relevant information. This includes the consideration of automated control activities around completeness, accuracy, restricted access, and validity of the data and information generated.

• The third phase involved training and users on techniques for effective input and extraction of information and reports from the data warehouse using reporting tools.

• The final phase involved designing and implementing operating procedures and control activities over the data warehouse and reporting tools to ensure completeness, accuracy, restricted access, and validity of the data and information input and reports generated.

• As a result of the project, the food distributor has a well-defined inventory of reports, improved data, and a more efficient process for capturing and using information for external financial reporting.
ICEFR Compendium
Example: Data Capture and Processing for Purchasing and Payables Cycle

• A publishing company recently implemented the purchasing and payables module of its existing ERP system. The key goals were to improve data quality, reduce manual handoffs through automation, and improve information flow/visibility into purchasing transactions.

• The implementation project team was lead by the controller, and supported by employees involved in the purchase to payables process. Workshops were held to confirm the current end to end process and identify important information about sources of transactions, key data requirements, risks to financial reporting, and information required for accounting and reporting.

• The project team used the results from these workshops to review the ERP module’s capabilities for automating tasks and controls such as:
  • Checking that data input was valid, complete, and accurate
  • Passing data between related transactions to minimize data entry and improve data consistency
  • Automatically recording the accounting transaction upon data input
  • Automatically reconciling the payables subsidiary ledger to the general ledger
  • Generating exception and analytical reports

• The result was access to more accurate, complete, and timely information for internal control purposes.
ICEFR Compendium
Approach: Enhancing Information Quality through a Data Governance Program

Senior management establishes a data governance program to support the company’s objectives of ensuring reliability of information used in support of internal controls and external financial reporting. Senior management formalizes policies, procedures, and responsibilities for data and information management considering the volume, complexity, and demand for rapid capture and dissemination from multiple sources. The data governance program includes policies and procedures for:

• Assigning roles and responsibilities between a central data management group, business functions, and IT
• Validating sources of information
• Establishing data-quality requirements before accepting sources into the information system
• Accessing rights to underlying data and related information produced through processing
• Protecting data during transmission and storage
Control Activities Principle 10: Selects and Develops Control Activities

“The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.”

Points of Focus:
- Integrates with Risk Assessment
- Considers Entity-Specific Factors
- Determines Relevant Business Processes
- Evaluates a Mix of Control Activity Types
- Considers at What Level Control Activities are Applied
- Addresses Segregation of Duties

Enhanced Aspects of Principle 10:
- Linkage between risk assessment and control activities
- Consideration of the level at which control activities are applied
- The types of controls applied (considering preventative vs. detective controls)
- Differentiates between business process control activities and transaction control activities
## ICEFR Compendium

### Principle 10: Selects and Develops Control Activities

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Using Matrices, Workshops, or an Inventory of Control Activities to Map Identified Risks to Control Activities</td>
<td>• Using Workshops to Map Identified Risks to Control Activities</td>
</tr>
<tr>
<td>• Implementing or Assessing Control Activities When Outsourcing to a Third Party</td>
<td>• Using a Risk and Controls Matrix to Map Risks to Control Activities</td>
</tr>
<tr>
<td></td>
<td>• Using an Inventory of Risks and Control Activities</td>
</tr>
<tr>
<td>• Considering the Types of Control Activities</td>
<td>• Obtaining a Report on Controls from a Service Payroll Provider</td>
</tr>
<tr>
<td></td>
<td>• Implementing or Assessing Control Activities when a Report on Controls at a Service Provider is Not Available</td>
</tr>
<tr>
<td></td>
<td>• Balancing the Types of Control Activities</td>
</tr>
<tr>
<td></td>
<td>• Evaluating Preventative vs. Detective Control Activities</td>
</tr>
<tr>
<td></td>
<td>• Setting the Threshold for Business Process Reviews</td>
</tr>
<tr>
<td></td>
<td>• Controlling Significant Accounting Estimates</td>
</tr>
<tr>
<td></td>
<td>• Automating Balance Sheet Reconciliations</td>
</tr>
</tbody>
</table>
### ICEFR Compendium

**Principle 10: Selects and Develops Control Activities**

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Considering Alternative Control Activities to the Segregation of Duties</td>
<td>• Using Alternative Control Activities when Access to Purchasing Transactions Are Not Segregated</td>
</tr>
</tbody>
</table>
| • Identifying Incompatible Functions | • Manually Assessing Incompatible Functions Across an Entity  
    • Using Automated Tools to Enforce the Segregation of Incompatible Functions |
ICEFR Compendium

Approach: Implementing or Assessing Control Activities When Outsourcing to a Third Party

- The organization outsources some of its operations to a third party.
- Management obtains an understanding of the service organization’s activities and whether those activities impact significant classes of transactions, accounts, or disclosures in the company’s reporting process. In doing so, the entity considers:
  - Significance of transactions or information processed in relation to the F/S
  - Risk of material omission and misstatement associated with assertions affected
  - Nature and complexity of the services provided and whether highly standardized and used extensively
  - Extent to which entity’s processes and control activities interact with those of the service organization
  - Entity’s control activities applied to the transactions affected
  - Terms of the contract with the service provider

If management determines service organization’s processes are significant to ICEFR, then it:
- Identifies the specific control activities performed by the OSP
- Selects and develops control activities internally over activities of OSP
Monitoring Activities Principle 16
Conducts Ongoing and/or Separate Evaluations

“The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning”

Points of Focus:

• Considers a mix of ongoing and separate evaluations
• Considers rate of change
• Establishes baseline understanding
• Uses knowledgeable personnel
• Integrates with business processes
• Adjusts scope and frequency
• Objectively evaluates
## Monitoring Activities Principle 16
Conducts Ongoing and/or Separate Evaluations

### Enhanced Aspects of Principle 16:

- Considering the rate of change when developing monitoring activities
- Using a baseline of understanding of internal control to establish plans for ongoing and separate evaluations
- Considerations regarding monitoring at different levels of an organization and monitoring of outsourced service providers
- Using technology in the context of monitoring
### ICEFR Compendium

**Principle 16: Conducts Ongoing and/or Separate Evaluations**

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Periodically Reviewing the Mix of Monitoring Activities</td>
<td>• Changes in Business Operations</td>
</tr>
<tr>
<td>• Establishing a Baseline</td>
<td>• Changing the Internal Audit Plan</td>
</tr>
<tr>
<td>• Identifying and Using Metrics</td>
<td>• Establishing a Baseline</td>
</tr>
<tr>
<td>• Designing and Implementing a Dashboard</td>
<td>• Using Metrics to Monitor Payroll</td>
</tr>
<tr>
<td></td>
<td>• Using Built-in Operating Measures and Key Control Indicators</td>
</tr>
<tr>
<td></td>
<td>• Using Dashboards to Relate Operating Information</td>
</tr>
</tbody>
</table>
# ICEFR Compendium

## Principle 16: Conducts Ongoing and/or Separate Evaluations

<table>
<thead>
<tr>
<th>ICEFR Approaches</th>
<th>ICEFR Examples</th>
</tr>
</thead>
</table>
| • Using Technology to Support Monitoring Activities | • Using Continuous Monitoring  
|                  | • Using Technology to Identify Trends |
| • Conducting Separate Evaluations | • Investigating and Reporting Whistle-blower Allegations  
|                                  | • Identifying and Protecting Sensitive Financial Data and Information  
|                                  | • Conducting Senior Financial Officer Visits  
|                                  | • Using Self-Assessments |
| • Using Internal Audit to Conduct Separate Evaluations | • Identifying and Analyzing Risk of Material Omission of Misstatement Due to Fraud  
|                                                           | • Internal Audit Conducting Separate Evaluations |
| • Understanding Controls at an Outsourced Service Provider | • Reviewing Service Auditor’s Report for Changes in Controls |
Management obtains and reviews periodic information from outsourced service providers to detect any changes in activities that impact the entity’s system of internal control over external financial reporting. Information obtained may include:

- The outsourced service provider’s applicable control objectives
- Details about which of the outsourced service provider’s internal control have been examined and included in any report
- The details and results from any independent audit testing performed
- Special considerations for the outsourced service provider that impacts the report

To determine what impact any identified changes may have on the entity’s system of internal control over external financial reporting, the following may also be assessed:

- Known changes in business processes
- Whether any exceptions were noted that may trigger further review
- Whether management is satisfied with the independence and objectivity of the report

Based on management’s review and findings, it may be necessary to reassess the separate evaluation activities over the outsourced service provider.
A supplies materials company has outsourced its payroll activities for a number of years to reputable payroll service provider.

The chief audit executive obtains an annual service auditor’s report detailing the internal controls at the service provider and compares the current report to past reports to determine if there are changes in relevant controls that could impact judgments made on planned monitoring activities over the payroll process.

The current report indicates some key changes in the payroll service provider’s software and several negative test results in priority risk areas. As a result, the CAE has the internal audit department perform a reconciliation of the payroll service provider’s processing results to evaluate if additional separate evaluations of the payroll service provider may be necessary.