Information Risk Management: Automated Control and Continuous Monitoring

April, 2012
Agenda

- Information Risk Context
- Information Control Types
- Information Control and Continuous Auditing Cases
- Information Control Working Session
- Next Steps
Risk Context
Balancing Act Between Operations, Risk and Control
Risk Management Options

- **Accept**: Accept at present level, Reprice, Self insure, Offset
- **Reduce**: Accept, Reject
- **Transfer**: Avoid, Control
- **Avoid**: Reduce
- **Retain**: Control
COSO Enterprise Risk Management Framework

Ref: COSO ERM, 2004

Ref: COSO Internal Control Framework, 1992
COBIT – Framework

Criteria
- Effectiveness
- Efficiency
- Confidenciality
- Integrity
- Availability
- Compliance
- Reliability

Business Objectives

IT RESOURCES
- Data
- Application systems
- Technology
- Facilities
- People

PLAN AND ORGANIZE

ACQUIRE AND IMPLEMENT

DELIVER AND SUPPORT

MONITOR AND EVALUATE

Source: ISACA, 2007
### Risk

Risk is defined as the chance of something happening that will have a negative impact upon an organization’s objectives and related assets.

### Control

Information based routines or procedure which senior management uses to alter or maintain patterns in organizational activities.

### KRI

A measurement, observed or calculated, indicates the presence or state of a condition or trend regarding certain risk.
Information Control Types
Information Control Universe

- Inter-Application Control
- Application Control
- Financial and Accounting Control
- Transaction Control
- Management and Administrative Controls
- Corporate Policy and Governance Controls

Ref: CICA
Application Controls

- General Controls
  - Segregation of duties
  - Software approval
  - Software change approval and change controls
  - Data base administration
  - Access and machine controls

- Information Controls
  - Input controls
  - Processing controls
  - Output controls
  - Error correction controls
Inter Application Controls

1. Does a control verify that total number of records that passed out of application A actually made it into application B?
2. Does the total amount of record or transaction value sent from application A match the amount received by application B?
3. Is there a consistent and independent process by which each of the detailed line items between the two sources were reconciled?
4. Does the control system detect the presence of duplicate transactions?
5. Does it detect the case where a file provided by application A is never processed by application B?
6. Did all of the information that application A sent to application B make it into application B within an expected amount of time?
Transaction Controls

- Integrity of Transactions
- Path of Transactions
- Timeliness of Transactions
- Exception Management
Finance and Accounting Controls

Application A ➔ Assets ➔ GL ➔ Internal Reports
Application B ➔ Liabilities ➔ GL ➔ Internal Reports
Application C ➔ Income ➔ Internal Reports
Application D ➔ GL ➔ External Reports
Application E ➔ GL ➔ External Reports

Internal Reports ➔ External Reports
Hierarchy of Controls

- Break complex checks into smaller, more manageable pieces
  - Low-level
  - Mid-level
  - High-level
  - Transaction
  - Account
  - Portfolio/client

- Consider the level when analyzing the best control for the situation
  - High-level controls: affect the largest number of processes
  - Mid-level controls: required for more detail processing, after high-level controls are performed
  - Low-level controls: required for verifying lowest level of detail

Source: Infogix Conference, 2007
Deterministic Information Control Portfolio

- **Verify**
  - Reasonability
  - Completeness
  - Content
  - Cross Reference
  - Duplicate

- **Balance**
  - Report-to-Report
  - Transaction Balancing
  - Run-to-Run
  - App-to-App
  - Real-Time, Batch

- **Reconcile**
  - Aggregate / Detail
  - One-to-One
  - One-to-Many
  - Many-to-Many
  - Suspense & Aging

- **Track**
  - Process Time
  - Process Delay
  - Process Sequence
  - Process Path
  - Process Integrity

Infogix
Verification | Working Example

- External system
- Commission feed
  - C1
  - C2
- Database
- Edits and Audits
  - Agent control file
  - Invalid records
  - Valid records
  - Month to date file
  - Sorting and Merging process
  - Counter of valid records
- Month to date file
- At the end of the month sent to the commission
Balancing | Working Example

External system → Commission feed → Edits and Audits → Invalid records → Counter of valid records

Agent control file → Invalid records

Valid records → Sorting and Merging process → Month to date file

Month to date file → At the end of the month sent to the commission

Database

C3

C4
Reconciliation | Working Example

External system

Commission feed

Edits and Audits

Agent control file

Invalid records

Valid records

Sorting and Merging process

Month to date file

Month to date file

Counter of valid records

Database

At the end of the month sent to the commission

C5
Tracking | Working Example

External system

Commissio

Edits and
Audits

Counter of
valid records

Agent
control file

Invalid
records

Valid
records

Month to
date file

Sorting and Merging
process

Month to
date file

At the end of the month sent
to the commission

Database

C6
# Statistical Information Control Portfolio

## Temporal
- Shewhart's Control Chart
- Reasonability
- Range / Outliers

## Spatial
- Gaps
- Benford's Law
- Duplicate / Split

## Ratio
- Benchmarking
- Min/Max ratio analysis
- Max/Max 2 ratio analysis
Application of Controls in Real world
Information Risk Scenarios in Business

- Transaction Processing Risk
- External Information Exchange Risk
- Financial Reporting Risk
- Fraud Risk
- Data Integrity of the risk reporting warehouse
Transaction Processing Risk

- **Example Processes**
  - Orders, Settlement
  - ATM, Deposit
  - Inter system verification
  - Money Movement

- **Risks**
  - Lost Message ~ Lost Revenue, customer complaints, rework
  - Delayed Message ~ SLA Fines, rework

- **Controls**
  - Real-time, end-to-end balancing and reconciliation
  - Real-time message tracking
External Information Exchange

- File #1
- File #2
- File #494
- File # 495

- Gateway

- Payment Processor
- Data

- Risks
  - Incomplete Transaction
  - Dropped Transaction
  - SLA violation

- Controls
  - Source system balancing
  - Dropped transaction monitoring
  - Error profiling
Financial Reporting Risk | GL Reconciliation | An Example in Use

- Adjustments/Additions
  - Non Systematic Accounts
  - Tickets
- Commercial Loans
- Principal Balance Check
- Principal Balance Check
- Duplicate Check, Principal Balance Check
- Subsidiary General Ledger
- LOB Data Warehouse
- Principal Balance Check
- Record Count Check
- Aggregate Balance Check
- Company Data Warehouse
- Parent Company General Ledger
- GAAP Reporting
- Regulatory Reporting
- Performance report
Fraud Risk

- Policy System
  - Detect Fraudulent Policy
- Claims System
  - Detect Invalid Claims
  - Detect Fraudulent Claims
- Commission System
  - Detect Fraudulent Commissions
- Accounts Payable System
  - Detect Duplicate Invoices
  - Detect unauthorized T&E expenses
## Data Warehouse Information Risk

### Risks
- Lost data during ETL process
- Limited traceability

### Controls
- Validate completeness of ETL loads into ERM DW
- Verify transformations during ETL process
- Assure correctness of ERM data
- Verifiable audit trails of testing and test cases
Information Risk Assessment and Auditing
A leading financial services processing company receives approximately 10 million transactions (using flat files) from its various branches. The transactions are processed each night to update customer’s accounts and financial systems.

One key challenge is to validate the integrity of all incoming information. There are incidents when certain incoming information is not accounted for resulting in customer complaints. In addition, certain transactions are accounted for twice which results in financial loss and in certain cases, customer dissatisfaction.

A Information Controls Assessment was recommended to identify areas where Information Controls may be deployed to mitigate the above risks.
How to ensure the Integrity of Transaction Information within Incoming Files?
How to ensure that all expected files have arrived?
How to ensure that no duplicate file has arrived?

Stores the financial information such as revenue and expenses etc.

How to ensure that the financial information is recorded appropriately

How to ensure that all incoming transactions are recorded appropriately

How to ensure that all incoming transactions are recorded appropriately and reconcile with the financial system

How to ensure that the customer information is recorded appropriately

Update customer specific information

Files Delivered to Processing Server → Staging Area → Staging Area II → Process 1 → Process 2 → CRM system → Financial System
High Level Control Recommendation

Files Delivered to Processing Server → Staging Area

- Check the integrity of incoming files. Validates that the information in the detail records (e.g. number of records, total amount) matches with the trailer data of the same file.
- Detect duplicate files
- Do an attendance check to ensure all expected files have arrived

Staging Area → Staging Area II

- Stores the financial information such as revenue and expenses etc.

Staging Area II → CRM system

- Update customer specific information
- Reconcile the number of records and dollar value of the transactions between the staging area and the CRM system
- Validate that CRM system was updated properly. Current balance = Previous balance + changes

CRM system → Process 1

Process 1 → Process 2

- Reconcile the number of records and transformed dollar value of the transactions between the CRM and the financial systems

Process 2 → Financial System

- Validate that financial system was updated properly. Current balance = Previous balance + changes
Information Controls Assessment Exercise

Distribute Handout to Audience
Information Controls Assessment Solution

Distribute Solution Set to Audience
Information Risk is pervasive

Information Risk Exposure can be identified through structured methodology

Information Risk can be managed through Automated Controls

Information Controls needs to be audited periodically since Information Risk profile changes with time