Integrated Audit Approach
An Overview

Monique Garsoux, Dexia
Qualified Audit Partners

RTM 22/01/2005
Presentation Outline

- The Need for Enterprises
- What is Integrated Auditing
- The integrated audit process – Audit methodology
- Best practices
Where are My Business Risks?
What is the Business problem?

Banksys

BANKS

Bank Statements
Where is the integrated audit approach (IAA)?
An example

- Operations
- Interest calculations
- Problem management
- Batch
- Branches
- Asynchrone
- Dialog Appl
- Banksys
- MQM
- Client Orders DB
- Accounting
- Account Orders Management
- Reconciliation
- CRE
- CRI
- Synchrone
- Security
- Oracle DB2
- Compliance
- Cics
- Network
What is Integrated Auditing

- Combines elements of three traditional audit types; Information technology (IT), operational and financial.

- Provides a broader audit scope in which to render an opinion on the adequacy and effectiveness of a system of internal control to mitigate global business risks: One report
Benefits of IAA

- Eliminates redundant or narrow view audits, Duplicated work, Missed opportunities for contribution, Risk of false assurance
- Creates a broad based audit.
- Examines global process risks.
- Provides Executives with a coherent view
- Once adopted, subsequent audits become highly efficient, focusing risks
- Combines what people do with what the computer does (or the contrary)
Effects of Technology

- Technology makes certain traditional audit procedures invalid and/or of limited value
- Transaction processing becomes automatic & invisible with reduced oversight due to less manual intervention
- New products / services / competition
Elements of IAA

- Examines the combined manual procedures that people use with “invisible” procedures that computers perform in the following steps impacts on:
  - Planning.
  - Evaluation.
  - Testing.
  - Reporting.
  - Follow-up.
Effect of traditional approach on the Audit Process

- Uncoordinated audit plans
- Separate audits
- Parallel audits; two or more distinct audits
- Concurrent audits; risk analysis initiatives, process reengineering, performed around the same timeframe
Results of Auditor’s Response

- Specialization & Silo Auditing
- Staff segregation between IT and Financial - Operational
- “The wall” erected within audit departments
IAA Audit Planning

- **IAA critical success factor:**
  For each critical Potential Process, identify the IT system that supports the activities. For each business activity (main business functions), identify critical system, interfaces, key manual procedures, especially reconciliations, and General Ledger impact.

- Coordinate efforts
IAA Planning

- IAA pitfall to avoid:
  - Not identifying IT components.
  - Not involving/confirming with Potential Audit Client management.
  - Not identifying manual “work arounds”; processes that take place outside of the normal process flow.
  - Not taking enough time to plan.
IAA Planning

- IAA planning should also identify for each Potential Audit Client (Processes) and related IT system:
  - Master Files.
  - System connectivity.
  - Sensitive/confidential data.
  - Information output; reports, computer generated transactions, and computer-to-computer transmissions.
IAA Planning

- Based on criticality ranking, select audit missions
- Result is coordinated audit plan where audit missions have been documented by an overview understanding of the subject
IAA Evaluation

- Depending on the scope of the audits selected (entire Potential Audit Client, one or more business activities), the auditor will “drill down” to obtain more detailed understanding of the specific controls related to the Potential Audit Client or business activity under review.

- Where necessary (based on potential risks)
IAA Evaluation

- IAA evaluation consists of obtaining a detailed understanding of the control environment design; “Do adequate controls exist” to mitigate business risks (scope selected based on risks)
IAA Evaluation – Risk Assessment

- IAA critical success factor – control design MUST include operational and IT controls.

- TOTAL risk assessment incorporates business/industry risk, operational risk COMBINED with technology risk to form an opinion on the overall design of controls.
Where are the risks?

- Operations
- Interest calculations
- Problem management
- Batch
- Account Orders Management
- Asynchrone
- Dialog Appl
- Synchrone
- Client Orders DB
- Accounting
- Reconciliation
- CRE
- CRI
- Integrated Audit
- MQM
- Banksys
- Network
- Security
- Oracle DB2
- Compliance
IAA Evaluation

IAA risk assessment guidelines:

- A limited number of risk factors
- Including Business - Technology specific.
- Risk factors should be weighted by criticality and measurable.
- Some factors should be IT specific.
IAA - Integrated Risk Assessment

- For EACH business unit, identify technology platform (PC, LAN, etc)
- “What does the system do?”
- Interview users, read documentation, look at system menu
- “What are you connected to?” - Interfaces
- Establishes span of control
IAA - Integrated Risk Assessment

- What could go wrong?
- Establishes the risk
- What would happen?
- Establishes the materiality
- “How would you know if something went wrong?”
- Determines the control
Integrated Risk Assessment

- Business criticality – degree of reliance a business Unit places on the system
- Technological complexity – degree of computer generated transactions utilized with minimal manual intervention
IAA Evaluation

Based upon the information obtained and confirmed during the planning phase, combined with the combined risk assessment, the auditor selects the relevant areas to include in the audit scope and performs a detailed review of these areas.
IAA Evaluation

- Auditors usually perform a walkthrough during the evaluation to assist in understanding the process flow, obtain relevant sample documentation, spot test the key controls, and observe the general environment.
IAA Evaluation

- IAA critical success factor – the auditor must flowchart the IT system to obtain a detailed understanding of key system processes, files and controls.
IAA Evaluation

- The auditor should develop an integrated flow chart that combines manual and computer processes, key calculations, master file updates, downloads, and uploads.

- Examine processes and control design by splitting them into three categories:
  - Those that only people perform.
  - Those that people and computers perform.
  - Those that only the computer performs.
1. DEMANDE D'ABONNEMENT VIA AGENCE

**Input**
- Demande d'abonnement signée

**Data**
- GEKT Abonnement en attente de recyclage / examen
- Code rejet

**Process**
- GEKT contrôle filtres validité abonnement
- Batch Journalier
- Online Encodage GEKT - contrôle online des filtres et autorisation sur compte
- Autorisation - Accès Controles Exhaustivité
- Intégrité Convivialité

**Output**
- Lettre N° Abonnement si pas premier abonnement
- intergité interception perte
- OUI
- Abonnement OK ?
- Rejet temporaire
- Code secret encrypté
- Confidentialité Intégrité
- batch
- Génération code secret
- Algorithme fort Sécurité

**Data**
- Liste des rejets Messages d'erreur à examiner
- délai intégrité

**Process**
- Batch
- Input
- Output
- Lettre Code Secret (le lendemain si 2 ième abo)
IAA Evaluation

Examine the following objectives for each transaction

- Completeness of input processing.
- Accuracy of input processing.
- Completeness of master file updates.
- Accuracy of master file updates.
- Accuracy and reliability of processing (calculations)
- Access to and confidentiality of information.
- Authorization of processing.
- Reconciliations and verifications.
- Monitoring and oversight.
IAA Evaluation

- Based on the evaluation of the design of the entire control environment (IT and manual), the auditor expresses an opinion on the “adequacy” of control design.
IAA Evaluation

- Audit approach - evaluation
  - What does the system do?
  - What is it connected to?
  - Who has access?
  - What type of access do they have?
  - What is logged?
IAA Evaluation

- Evaluation
  - Totals (completeness)
  - Edits (accuracy)
  - System generated calculations/summarization/categorization
  - System menu
IAA Evaluation

- Better evaluation
  - Transaction file - input - journal
  - Master file - processing - ledger
  - “Master file update”
  - “How do you know”
IAA Testing

- The testing phase is the area that makes the IAA the most efficient.
- Based on the information obtained in planning and evaluation, the auditor selects which controls require testing.
IAA Testing

- Better audit tests
  - On screen edits
  - Batch totals
  - Calculations
  - Master file updates
  - Output
IAA Testing

- Better audit tests
  - System demo
  - Access
  - Violations
  - Computer generated logs/listings
IAA Reporting

- Although reporting is largely a matter of preference and style, IAA reporting has certain benefits that can be incorporated into any reporting style: a single report that renders an opinion on the entire system of risks and control.

- Visual = no long narrative texts
IAA Reporting

IAA pitfall to avoid - reporting that is done by a technical auditor and a non-technical auditor and then pieced together. This tends to mitigate the consistency of ideas. Judicious editing is required to scrub the report to eliminate jargon and facilitate easy reading.
IAA Hitting the High Spots

- Application audits
  - Transaction processing
  - Business critical
  - ”Bread and butter”
EXPECTATIONS

- Depends on ...
  - DUE DILIGENCE AUDIT MODEL?
  - STAFFING AND DEVELOPMENT AUDIT MODEL?
  - PROFESSIONAL INTERNAL AUDIT MODEL?
WHAT WORKS

- Expanding the information technology knowledge base of each and every auditor
- Realistic audit assignments based on knowledge, skill levels and degree of difficulty of the subject (planning audits)
- Pre-audit of technical aspects (typical IT audits)
- Extensive IT audit tools and support
- Effective technical supervision
BARRIERS

- IT audit is a separate and unique audit discipline
- The fundamental internal auditor skill set is accounting and general business oriented with limited IT knowledge required
- Specialization is good – only IT auditors should audit IT topics
- Generalization is good – It auditors can audit anything IT related
- The board and senior management really understand auditing in an IT environment
- No one really cares whether audits are integrated or not
- Auditors are not on staff long enough to justify extensive training costs
IAA Integrated auditor?

- Traditional auditor that addresses computer audit techniques, rely on the methodology
- Specialized IT auditor that addresses both business flow and Highly automated systems
- All auditors integrated auditors with some having just more skills than others
IAA Audit Tools

- Reference materials
  - Cobit (Manage Data)
  - ISACA Bookstore material (bits and pieces in many books)
  - Integrated referential a real need ...

- Audit software ACL, IDEA
### PROCESS 1: Procédures d'introduction des données

<table>
<thead>
<tr>
<th>Objectif</th>
<th>Risques Potentiels</th>
<th>Contrôles</th>
<th>Risques résiduels et recommandations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management should establish data preparation procedures to be followed by user departments. In this context, input form design should help to assure that errors and omissions are minimised. Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.</td>
<td>Risque potentiel est l'introduction de crédits ou de placements</td>
<td>mes constatations</td>
<td>risque résiduel et recommandations</td>
</tr>
<tr>
<td>Management should ensure that source documents are properly prepared by authorised personnel who are acting within their authority and that an adequate segregation of duties is in place regarding the origination and approval of source documents.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The organisation's procedures should ensure that all authorised source documents are complete and accurate, properly accounted for and transmitted in a timely manner for entry.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error handling procedures during data origination should reasonably ensure that errors and irregularities are detected, reported and corrected.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures should be in place to ensure original source documents are retained or are reproducible by the organisation for an adequate amount of time to facilitate retrieval or reconstruction of data as well as to satisfy legal requirements.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The organisation should establish appropriate procedures to ensure that data input is performed only by authorised staff.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### PROCESS 1 : Caractère complet, correct et autorisé de l'introduction

<table>
<thead>
<tr>
<th>Objectif</th>
<th>Risques Potentiels</th>
<th>Contrôles</th>
<th>Risques résiduels et recommandations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Les données introduites doivent être validées le plus près possible du moment de la saisie</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### PROCESS 1 : Traitement des erreurs de saisie

<table>
<thead>
<tr>
<th>Objectif</th>
<th>Risques Potentiels</th>
<th>Contrôles</th>
<th>Risques résiduels et recommandations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Des procédures doivent être prévues pour la correction et la re-soumission des données incorrectes.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### PROCESS 1 : Validation dans le traitement de l'information

<table>
<thead>
<tr>
<th>Objectif</th>
<th>Risques Potentiels</th>
<th>Contrôles</th>
<th>Risques résiduels et recommandations</th>
</tr>
</thead>
<tbody>
<tr>
<td>The organisation should establish procedures to ensure that data processing validation, authentication and editing is performed as close to the point of origination as possible. When using Artificial Intelligence systems, these systems should be placed in an interactive control framework with human operators to ensure that vital decisions are approved. The organisation should establish procedures for the processing of data that ensure separation of duties is maintained and that work performed is routinely verified. The procedures should ensure adequate update controls such as run-to-run control totals and master file update controls are in place.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IAA Education

- On the field but ...
- Continuing education
  - Budget $$$
  - Established education vendors $$
  - Local IIA/ISACA chapters if...
  - In-house training if ...
  - Partner with other companies on-site... not commonly used
Discussion

- Question 1: The integrated auditor or a team of competencies?
- Question 2: How to create or upgrade the competence in integrated auditing