IT Audit at UBS - a Fully Integrated Approach

Gerd Lierhaus
Group Internal Audit, IT WM&SB

January 2011
Table of Contents

1. UBS Group Internal Audit
2. Former IT Audit Approach
3. UBS Group Internal Audit Process
4. Integrated IT Audit Approach
   • Example 1: Change Management
   • Example 2: Access Control
5. Benefits and challenges
6. Questions & Answers
Section 1

UBS Group Internal Audit
Locations of Group Internal Audit

Located in nine countries

Headcount as of 1 March 2010: 301.65 FTE / 308 people

- Asia Pacific: 13%
- Americas: 26%
- Europe: 23%
- CH: 38%
Audit involvement of IT WM&SB in 2011 (planning)

- IT led audits
  - Board of Directors (BoD): 10 of 13 in total; 1 lead
  - Cycle audits: 6 of 28; 4 leads

- Business led audits
  - WM&SB:12
  - EMEA: 9
  - Corporate Center: 6
Section 2

Former IT Audit Approach
Overview

- Pure IT audits
  - Focused on IT infrastructure
  - Very few IT process audits in the application area

- Integrated audits: covered IT Control Areas
  1. IT Strategy and Management
  2. System Processing and Business Processes
  3. System Security
  4. IT System Operations
  5. Business Contingency Planning
Characteristics of this approach

- Relatively independent planning of the major IT part
  - Difficult scoping for the general IT controls (GITC)

- Relatively independent fieldwork conduction
  - No interconnection for the GITC part
  - IT owned working paper

- Resulting in relatively independent IT issues on general IT controls
  - In case of issues with a general IT process
    - Risk of the issue not necessarily in the (business) focus of the audit
    - Addressees somewhere in the IT, maybe not even informed beforehand

- Weaknesses
  - Less acceptance by the business audit as 'added value' was not very high
  - Producing 'always' the same type of IT issues, e.g. on access control
  - Additional IT review cycles → extending reporting periods
  - Shift of scope from business to IT
  - Conflicts in the rating of issues respectively with the overall audit rating
Former Approach - Audit Process

PLANNING
Plan and design the audit approach

- Pre-plan
- Obtain background information
- Perform preliminary review of systems, processes, structures and procedures
- Understand internal control and assess control risk
- Define the audit plan and allocate resources

Fieldwork
Assess

- Effectiveness of risk management, control and governance processes
- Compliance with statutory, legal and regulatory requirements
- Reliability of information

- IT presents flow and testing at the end of WBS
- Walkthrough / WBS Opportunity

Evaluate internal control design effectiveness ("walkthroughs"

- Whiteboard

Evaluate internal control operating effectiveness ("tests of controls"

- Test Opportunity

- RCM
- WP
- SOI
- Results

Perform tests of details ("substantive tests"

- Workpaper Opportunity

- IT Reviews
- IT RCMs
- Biz Reviews
- Biz RCMs

REPORTING
Complete the audit and communicate the results

- Evaluate results
- Issue audit report
- ML draft
- Comments on ML draft
- Up-dated version of ML
- Evaluate results and make rating proposal
- High-level Report draft
- Get rating approval
- Comments on High-level Report
- Report issuance
- Completion Statement

Follow-up
Governance and Activity Reporting

Planning + Discussion Opportunity

IT Begins

Business Begins

IT Ends

Reporting Opportunity

Business Ends
Section 3

UBS Group Internal Audit Process
Risk-based audit execution with the "Thin Red Line" concept

The "Thin Red Line" is a concept of maintaining focus on the most important risks

- Clearly determined and communicated audit objectives
Risk-based audit testing approach

Risk-based testing approach

- Test and evaluate the design effectiveness
  - Walkthroughs
    - Design effective?
      - Yes, design effective
      - No, design ineffective
  - Analytical procedures to confirm the risk assessment (e.g. using CAATs, ACL, Access, Excel)
  - Other (e.g. Review of risk reports, policies etc.)

- Test and evaluate the operating effectiveness
  - Further testing necessary?
    - No
      - Not applicable
    - Yes
      - Further testing necessary?
        - Yes
          - Tests of controls
            - Weakness?
              - No control weakness
              - Control weakness
                - Tests of details (*tests of transactions*, *tests of balances*)
        - No
          - Evaluation and conclusion on design and operating effectiveness

Documentation

- WP (Walkthrough Tasks)
  - Whiteboard Session
- WP (Testing Tasks and Other Tasks)
- WP (Draft Issues List)
Section 4

Integrated IT Audit Approach
Integrated Approach - Audit Process

**PLANNING**

Plan and design the audit approach

- Pre-plan
- Obtain background information
- Perform preliminary review of systems, processes, structures and procedures

**FIELDWORK**

Assess effectiveness of risk management, control and governance processes

- ii) compliance with statutory, legal and regulatory requirements
- iii) reliability of information

- Evaluate internal control design effectiveness (*walkthroughs*)
- Evaluate internal control operating effectiveness (*tests of controls*)
- Perform tests of details (*substantive tests*)

- Whiteboard
- Enhanced AF & Data Testing

**REPORTING**

Complete the audit and communicate the results

- Evaluate results
- Issue audit report
- ML draft
- Comments on ML draft
- Up-dated version of ML
- Evaluate results and make rating proposal
- High-level Report draft
- Get rating approval
- Comments on High-level Report
- Report issuance

- Completion Statement
- Follow-up
- Governance and Activity Reporting

- Business Reviews
- Business & IT RCMs (and Work papers as necessary)

Begin research in advance of fieldwork - start to prepare for future meetings (proactive vs. reactive)

Attend initial kick off meetings with Business Manager (RA)

Attend relevant business walkthroughs to understand the F2B flow (IT impact)

Demo and obtain QA access to the applications of focus

At WBS, IT presents F2B flow and testing approach via business objective

- Engage with the RA and draft MLs in relation to their business context with clear impact / risk statements.
- Work with the RA to provide IT relevant context for the ES and Supplementary Business Information (SBI)

**Business and IT begins**
The IT integrated audit approach - principles of operation

- IT audit scope driven by the key audit objectives, whether these are business or technology related.

- Planning for integrated audits is done jointly, with IT and business auditors attending meetings with key business and Group Technology management.

- Walkthroughs are performed jointly to understand all aspects of the business and process flow.

- Whiteboards based on common process flow charts that reflect business and technology risks, aligned with the key audit objectives.

- IT fieldwork driven by key audit risks and focus on automated application controls and functionality – assess “fit for purpose”.

- Enhanced application functionality testing - CAATS, real system test scenarios, and review of logic (system, reporting, or exception handing)

- IT work papers and RCM components included under the business RCM sections: **no separate IT application working papers**

- Joint assessment of issues to reflect impact holistically: IT involvement in materiality assessment and drafting of the audit report.
Example 1: Change Management – in an IT process audit

Assess the control effectiveness of the whole process

- Determine Key Risks in the process
- Evaluate the design of Key Controls
- Assess the operational effectiveness of these key controls in a sample testing
  - Sample within the IT function
  - Sample of IT projects – providing business functionality
Example 1: Change Management – in an integrated audit

Assess the operational effectiveness of business related Key Controls

1. Requirements Sign-off (RSO): Involvement of business as a key stakeholder
   - IT audit: including appropriate other necessary stakeholders

2. Production Sign-off (PSO): Approval provided by the business representative
   - IT audit: including necessary IT specific tests

3. Suitable Test Plan covering all business risks
   - IT audit: including necessary IT specific tests

4. Effective User Acceptance Testing (UAT)

Integrated approach

- All four key controls require business understanding
- Effective audit testing only with a close cooperation between IT and business audit
  - Business audit knows the responsibilities and business requirements and expected results
  - IT audit knows the process and tools; and IT specific responsibilities and requirements
Example 2: Access Control – in an IT process audit

Assess the control effectiveness of the whole process

- Determine Key Risks in the process
- Evaluate the design of Key Controls
- Assess the operational effectiveness of these key controls in a sample testing
  - Sample within the IT function
  - Sample of Business applications
Example 2: Access Control – in an integrated audit

Assess the operational effectiveness of business related Key Controls

1. Request assessment and approval: Appropriateness of approver chain

2. Periodical review: Actually conducted

3. Authorization concept: a) Reflecting business needs
   b) IT audit, in the management system: Access rights for administration roles
   c) IT audit, on application level: Actual implementation

Integrated approach

• All three key controls require business understanding
• Controls 1, 2 and 3a can be conducted by business without IT
• Control 3: parts b) and especially c) require IT audit know-how and skills but a control weakness here has a direct business impact
Section 5

Benefits and challenges
Benefits

• IT general controls mostly covered in themed reviews where there is more opportunity to assess holistically at the entity level and determine materiality

• Reduced IT general controls testing during integrated audits in order to maximize the application functionality testing approach – allow flexibility to test IT general controls if part of key audit objectives and risks.

• More communication between teams so that audit scope, objectives and responsibilities are transparent to the entire audit team involved in an integrated audit.

• Focus on the business process risks to determine application and IT testing

• Increased joint testing and facilitate improved understanding of the processing flows, whether business or IT.

• Increased use of CAATS, data mining and automated testing techniques.

• Ideally: no IT issues – but business issues on underlying IT controls
Challenges

- IT issue is NOT a weakness of operational effectiveness of the respective application but a design issue
  1. In the related IT process; or
  2. In a broader business context

Examples
- A PSO is not only not effectively conducted but the respective unit is not using the (audited) standard Change Management process
  → No effectively designed PSO; e.g. in a small international unit
- Access rights are not only not effectively assigned for the application in scope but the authorization concept for a whole bunch of related applications is not effectively designed

- Consequences
  - Assessment of a process necessary which is not in the scope of the audit
  - Decision to be made whether
    - Scope needs to be extended to address the full issue
    - Broader issue is handled separately
Audit Planning Activities

Instrument to deal with "Emerging risks": **Anticipatory Auditing**

- Targeted review
- New (unplanned) audit
Questions & Answers