IT Risk Assessments

SF ISACA Fall Conference

September 2003
Introductions

Enterprise Risk Services
- Kevin Fried – Partner
- Monica O’Reilly – Senior Manager
- Duy Nguyen – Manager

Participants
- Name
- Company
- Session objectives
Agenda

- Risk Assessment Overview
- IT Risk Assessment Objectives
- IT Risk Assessment Methodology
- IT Risk Assessment Tool
- Case Study
Applications of Risk Assessments

- Enterprise-wide Risk Assessment
- Specific Risk Assessment
- IT Risk Assessment
- Management Self Assessment
  - Key Performance Indicators
  - Continuous Monitoring
- Internal Audit Risk Assessment
- Financial Audit Risk Assessment
IT Risk Assessment Objectives

- Identify IT risks that may prevent the IT organization from achieving its business objectives – comprehensive risk identification is crucial for the development of risk mitigation strategies

- Develop and maintain an understanding of the IT environment (infrastructure and critical application systems)

- Identify issues and/or potential changes in the IT environment that result in new risks

- Obtain management’s input and consensus on goals, initiatives, risks and issues

- Develop a risk-based annual audit plan
Risk Assessment and Audit Plan Development

1. Data Gathering
   - Interview key management, board members, other personnel
   - Identify key business strategies, processes, activities, and risks
   - Review financial results, business plans, and prior internal audit reports
   - Identify business, industry, legislative, and regulatory issues
   - Compile industry leading practices

2. Assessment
   - Consider risk factors such as financial significance, control environment, regulatory compliance requirements, and systems reliance
   - Summarize results of business activity risk assessment
   - Develop audit universe
   - Prioritize audit universe topics based on significance and likelihood of occurrence

3. Plan Development
   - Develop proposed risk-based audit plan
   - Confirm conclusions with management and the Audit Committee
   - Finalize annual internal audit plan
Data Gathering

- Identify Potential Focus Areas (Technology Overview)
  - Location / Functional Units
  - Maturity of Technology
  - Maturity of IT Processes
  - Business Use / Criticality
  - Personnel Skill Level
  - Projects
- Review Relevant Reports and Industry Information
- Interview Key Management
Technology Overview

Core Business Systems
- Sales
- Manufacturing Systems
- ERP / Financials
- Customer Management

Administrative
- Human Resource
- Compliance
- Legal
- Product Quality

Reporting
- Management Portal
- Data Warehouses
- ERP Reporting

Infrastructure
- Access Control
- Change Control
- Hardware Environment
- Operating Systems
- Other
Review Reports and Industry Information

- Internal Audit Report
- External Audit Report
- IT Metrics
  - System availability
  - Outages and processing errors
  - Number and nature of changes
  - System usage and capacity
- Specific Research Studies and Reports (Gartner, etc.)
- Vendor Training
- Industry Benchmarking / Competitive Analysis / Market Trends
- Governmental & Regulatory Requirements
Interview Key Management

- CIO/CTO & Other Key IT Personnel
- Various Approaches for Conducting Interviews
  - Group vs. Individual Sessions
  - Anonymous Voting vs. Open Dialogue
  - Formal Questionnaires vs. Free Flowing Discussions
- Interview Questions (Discuss Risk Factors)
  - Current Goals & Objectives
  - Upcoming Changes
  - Risks for the Company
  - Risks in Meeting their Goals & Objectives
  - Internal Audit Experience & Expectations
- Document Results & Identify Common Themes
Assessment

- Evaluate Risk Factors
  - Financial Significance
  - Control environment
  - Regulatory Compliance

- Summarize Risks
  - Likelihood/Impact

- Define Audit Plan
- Develop Individual Audit Plans
Evaluate Risk Factors

Types of Risk (COSO Definitions)

- **Operational Risk** – Operational efficiencies and adherence to managerial policies; includes detailed operational control (systems & technologies, policies, staffing, product/process changes, business interruption)

- **Financial Risk** (volume, complexity, reporting, liquidity, safeguarding)
  - **Authorization** - There is proper authorization/segregation of duties.
  - **Recording** - Data is complete, accurate and recorded timely.
  - **Safeguard** - Assets are safeguarded.
  - **Reconciliation** - The accounts balance and reconcile and any differences are identified.

- **Regulatory / Compliance Risk** - The regulations, policies, and procedures governing the events and accounts are in place and being followed (law, regulations, compliance, special reporting, code of conduct, culture, ethics, self assessment, risk management activities)
Specific Risk Factors

Operational Risk Factors

- **Internal Controls** – Documented Policies & Procedures, Prior Year Audit Results, Overall Quality, Frequency, Last Time
- **Management & Key Personnel** – Turnover, Competence, Integrity, Morale
- **Department Goals & Objectives** – Performance Pressure, Consistency with Corporate Goals, Achievability, Competitive Pressure
- **Systems** – Age, Complexity, Automation, Changes, Decentralization, Importance
- **Business Risks** – Size of Operation, Decentralization, Importance, Complexity, Volume, Growth, Recent Performance

Financial Risks – Materiality (assets, revenue), Complexity, Volume

Regulations – Changes, Complexity, Industry Consideration
Summarize Risks

Quantitative vs. Qualitative Analysis

Quantitative
- Benefits - feels scientific, perceived as “more objective”, granularity of analysis
- Weaknesses - without weighted risk factors - results may be misleading

Qualitative
- Benefits – uses business / auditor judgment, less complicated and time-consuming
- Negative – consensus may be difficult

Our Recommendation
- Use a blended approach!!!
Summarize Risks

Likelihood and Impact Analysis

- **Likelihood**
  - Evaluate the likelihood of a negative impact occurring

- **Impact**
  - Evaluate the impact of the event occurring
Define Audit Plan

- **Priority**
  - Results from Risk Assessment
  - Board & Management Requests

- **Budget**
  - Individual Audit Budgets
  - Total Hours Available
  - Specialists Required
  - Departmental Skill Sets

- **Timing**
  - Implementation Dates
Develop Individual Audit Plans

- Evaluate Risk at a Lower Level
  - Review Documentation
  - Interview Lower Level Management
  - Evaluate Risk Factors

- Determine Scope & Objectives
  - End-to-End Audits
  - Risk Based Audits
  - Priority, Budget & Timing Considerations
New Assessment Information:

Assessment Name: This is a sample assessment

Company Name: XYZ Company

Division: Division 1

Industry: Energy Resources

Submit

Your Existing Assessments

<table>
<thead>
<tr>
<th>Assessment Name</th>
<th>Company</th>
<th>Created On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment 1</td>
<td>ABC Inc.</td>
<td>06/18/2003</td>
</tr>
<tr>
<td>Assessment 2</td>
<td>DEF Inc.</td>
<td>07/01/2003</td>
</tr>
<tr>
<td>Assessment 3</td>
<td>GHI Inc.</td>
<td>07/23/2003</td>
</tr>
<tr>
<td>Assessment 4</td>
<td>JKL Inc.</td>
<td>08/05/2003</td>
</tr>
<tr>
<td>Title</td>
<td>Date</td>
<td>Company</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Interview with Bob Lillard</td>
<td>08/15/2003</td>
<td>XYZ Company</td>
</tr>
<tr>
<td>Interview with Duc Nguyen</td>
<td>08/19/2003</td>
<td>XYZ Company</td>
</tr>
<tr>
<td>Interview with Greg Thomas</td>
<td>08/20/2003</td>
<td>XYZ Company</td>
</tr>
</tbody>
</table>
## Risk Assessment Input Screen:

**Company:** Company Name Here  
**Division:** Division Name Here  
**Date:** 12/1/2003  
**Interviewee:** Bob Smith  
**Title:** CIO XYZ Company

<table>
<thead>
<tr>
<th>Enterprise IT Risk Areas</th>
<th>Risk</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Strategy &amp; Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Human Resources</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Infrastructure &amp; Application Areas</th>
<th>Mainframe Risk</th>
<th>Mid-Range Risk</th>
<th>Network Risk</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Operations</td>
<td>H M L n/a</td>
<td>H M L n/a</td>
<td>H M L n/a</td>
<td></td>
</tr>
</tbody>
</table>

Deloitte & Touche
## Select Areas to Assess

**Assessment Name:** This is a sample IT assessment | **Created:** 9/15/2003 3:55:59 PM  
**Company:** XYZ Company | **Industry:** Retail/Consumer Products & Services

<table>
<thead>
<tr>
<th>Select</th>
<th>Select All the Process Areas That You Want to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>IT Governance</td>
</tr>
<tr>
<td>☐</td>
<td>IT Strategy and Planning</td>
</tr>
<tr>
<td>☐</td>
<td>Program Management</td>
</tr>
<tr>
<td>☐</td>
<td>Technology Management</td>
</tr>
<tr>
<td>☐</td>
<td>Operations</td>
</tr>
<tr>
<td>☐</td>
<td>Applications</td>
</tr>
<tr>
<td>☐</td>
<td>Support</td>
</tr>
<tr>
<td>☐</td>
<td>Enterprise Security Architecture and Management</td>
</tr>
<tr>
<td>☐</td>
<td>Business Continuity Management</td>
</tr>
<tr>
<td>☐</td>
<td>IT Human Resources</td>
</tr>
<tr>
<td>☐</td>
<td>IT Measurement &amp; Reporting</td>
</tr>
</tbody>
</table>

Submit
IT Process Assessment

Assessment Name: This is a sample IT assessment | Created: 9/16/2003 3:55:53 PM
Company: XYZ Company | Industry: Retail, Consumer Products & Services

Select an IT Performance Area to begin

<table>
<thead>
<tr>
<th>Performance Area</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td>Not Completed</td>
</tr>
<tr>
<td>Technology Management</td>
<td>Not Completed</td>
</tr>
<tr>
<td>Operations</td>
<td>In Progress</td>
</tr>
<tr>
<td>Applications</td>
<td>Not Completed</td>
</tr>
<tr>
<td>Support</td>
<td>Not Completed</td>
</tr>
<tr>
<td>Enterprise Security Architecture and Management</td>
<td>Not Completed</td>
</tr>
</tbody>
</table>
## IT Process Assessment

**Assessment Name:** This is a sample IT assessment | **Created:** 5/15/2003 3:55:03 PM  
**Company:** XYZ Company | **Industry:** Retail/Consumer Products & Services

**Area Selected:** Operations (0 Area Function(s) found)

### 1. Data Center Operations

- **Production Scheduling/Control**
  
  Q1. There are documented operations turnover procedures to manage transition between operations shifts and ensure resolution of problems that cross shift boundaries.
  
  Q2. Technologies such as production scheduling and resource scheduling tools are in place and used.
  
  Q3. There are guidelines and operations processes to prevent system resource conflicts and ensure the timely processing of all production workloads.
  
  Q4. Production control problems are documented, reported and acted upon.

- **Batch Processing**
  
  Q1. There are processes in place to ensure that batch processing does not exceed the batch processing window.
  
  Q2. Operations personnel have controls in place to throttle and regulate batch processing to avoid conflicts.
  
  Q3. There is a training program in place to train operations personnel on problem resolutions.
**IT Importance/Effectiveness Report (Level 1)**

**Company:** ABC Company  
**Assessment Name:** dnguyen  
**Created:** 4/1/2003 2:08:56 PM

**Overall Score:**

<table>
<thead>
<tr>
<th>IT Area (Click on Area for Area Detail)</th>
<th>Effectiveness Rating</th>
<th>Importance of Process</th>
<th>Exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Management</td>
<td></td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>IT Governance</td>
<td></td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>IT Strategy and Planning</td>
<td></td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>
### IT Importance/Effectiveness Report

**Company:** ABC Company  
**Assessment Name:** Example Assessment  
**Created:** 4/1/2003 2:00 58 PM  
Survey Industry: Energy Resources

Would you like to view a comparison with ALL Industries? Click HERE.

<table>
<thead>
<tr>
<th>IT Area</th>
<th>Survey Effectiveness Rating</th>
<th>Industry Effectiveness Rating (Energy Resources)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Strategy and Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Printable Version]  [Download/View in Excel]  [Download/View in Word]
Case Study

ABC Company IT Risk Assessment
ABC Company Profile

Company Background

- ABC Hotels & Resorts ("ABC") is a subsidiary of ABC PLC of the United Kingdom.
- ABC is a global leader in the hotel industry, operating over 2,700 hotels in 95 countries through franchising, ownership, management, and leasing.
- The ABC family of hotels is comprised of:
  - Grand Vacation
  - Holiday Express
  - Royal Plaza
  - Stoneridge Suites
  - Inter-Continental
- In 2002, ABC posted revenues of $1.9 billion, which represented a 36% increase over 2001 revenues.
- ABC’s operating profit on its 2002 revenue was $521 million, up $92 million from 2001.
ABC Information Technology Profile

Information Systems Background

- ABC has a diverse and complex information system infrastructure that has the following primary components:
  - The IT infrastructure is comprised of mainframe, Unix, and Windows NT elements.

- ABC’s North American data center located in Alpharetta, GA, is responsible for maintaining hotel and resort connectivity.
  - A full suite of PeopleSoft products, including Financials, Human Resources, and Payroll, has been implemented.
  - The TPF Reservation system has recently been deployed.
  - ABC utilizes an Oracle-based data warehouse.
  - An in-house developed reservation system is used for room rentals, marketing, and financial applications.
  - ABC is piloting wireless PDA technology for executive management
Q&A

Contact Information

- Kevin Fried 415-783-4639
- Monica O’Reilly 415-783-5780
- Duy Nguyen 415-783-4237