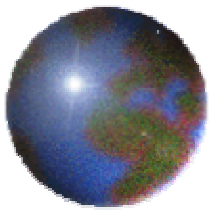


IT Risk Assessments

SF ISACA Fall Conference

September 2003

Deloitte & Touche

Introductions

Enterprise Risk Services

- Kevin Fried – Partner
- Monica O'Reilly – Senior Manager
- Duy Nguyen – Manager

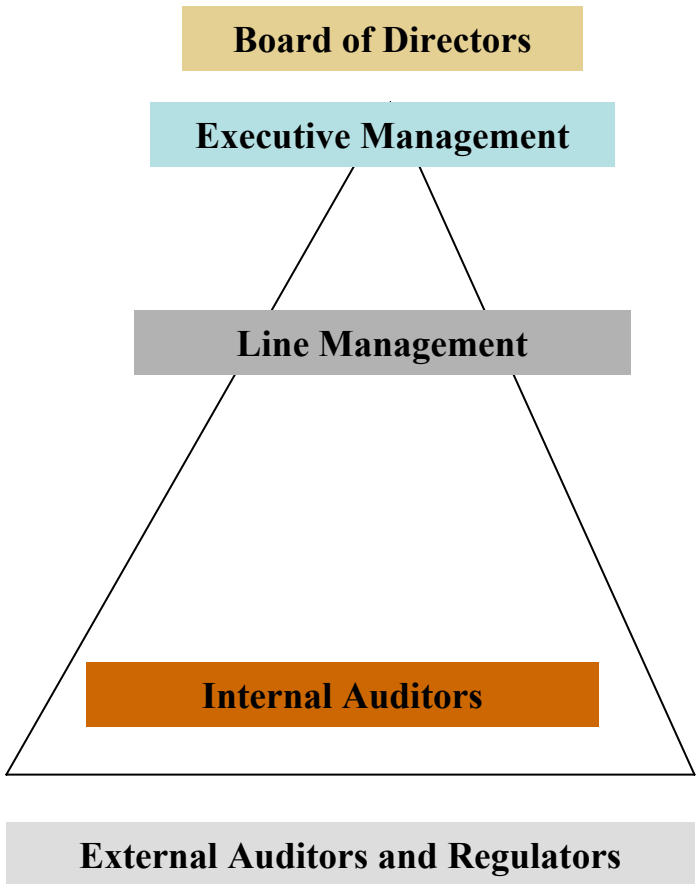
Participants

- 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



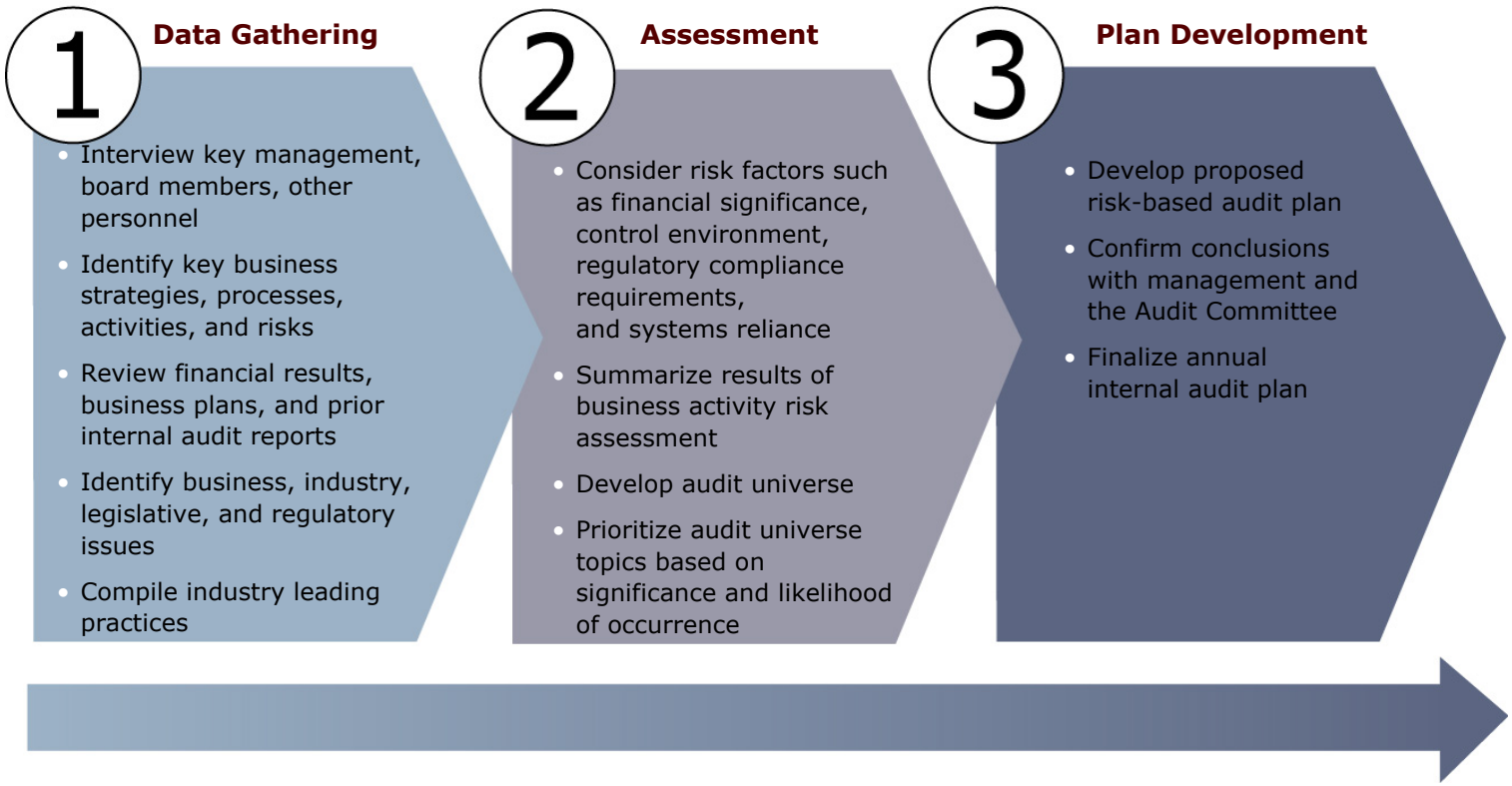
- Enterprise-wide Risk Assessment
- Specific Risk Assessment
- IT Risk Assessment
- Management Self Assessment
- Control Self Assessment
  - Key Performance Indicators
  - Continuous Monitoring
- Internal Audit Risk Assessment
- Financial Audit Risk Assessment

Deloitte & Touche

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

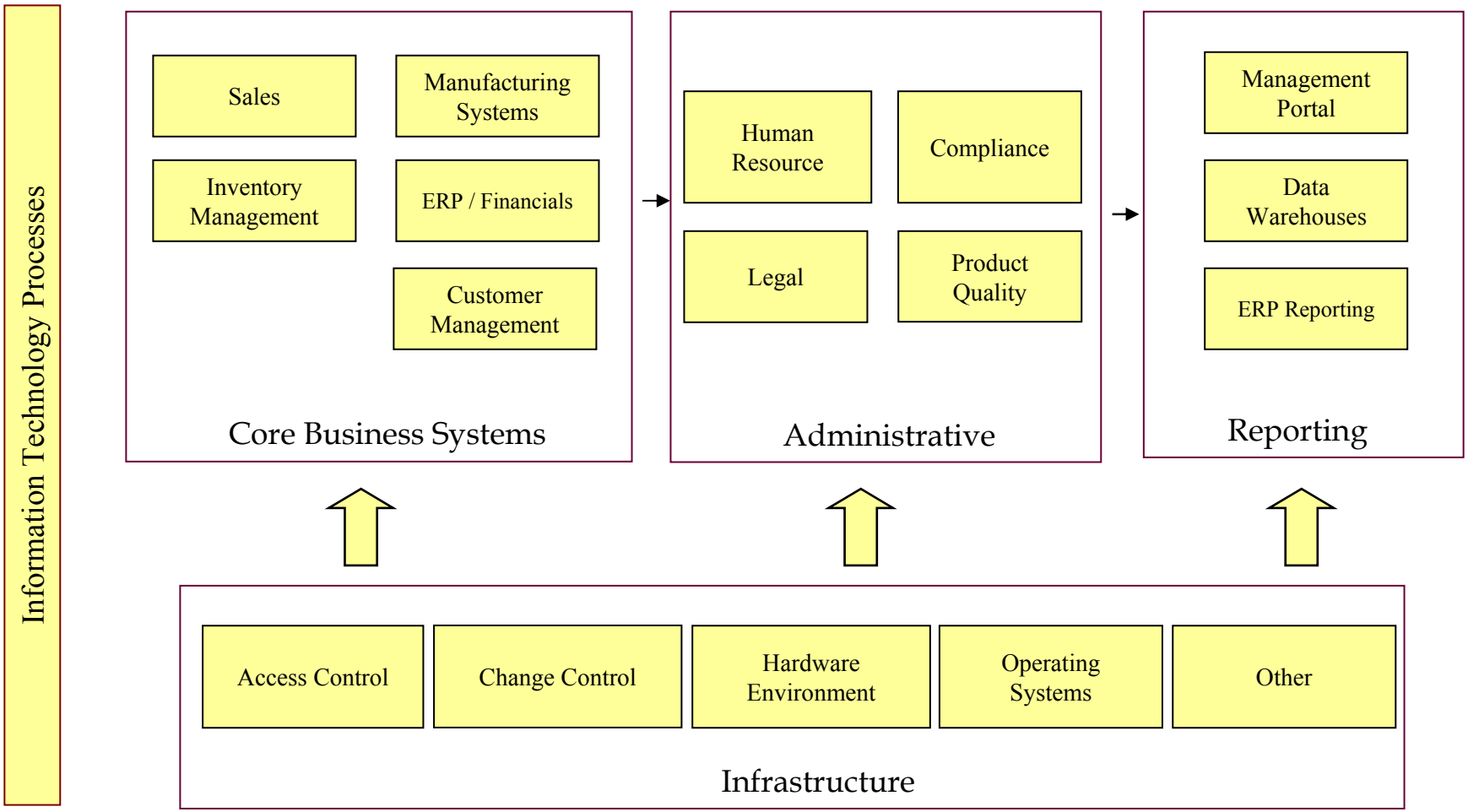


Deloitte & Touche

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



Deloitte & Touche

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

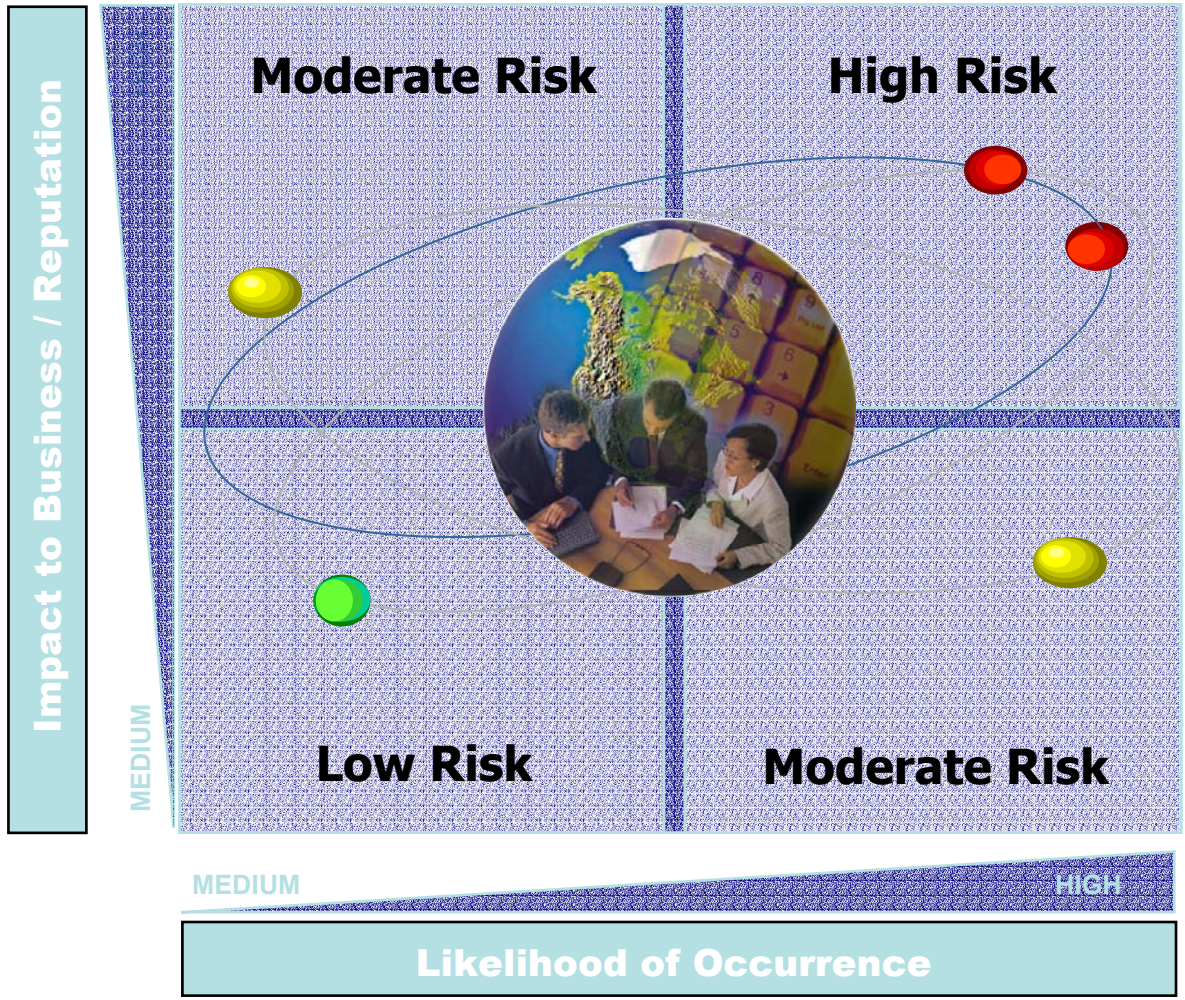
Quantitative vs. Qualitative Analysis

- 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



Deloitte & Touche

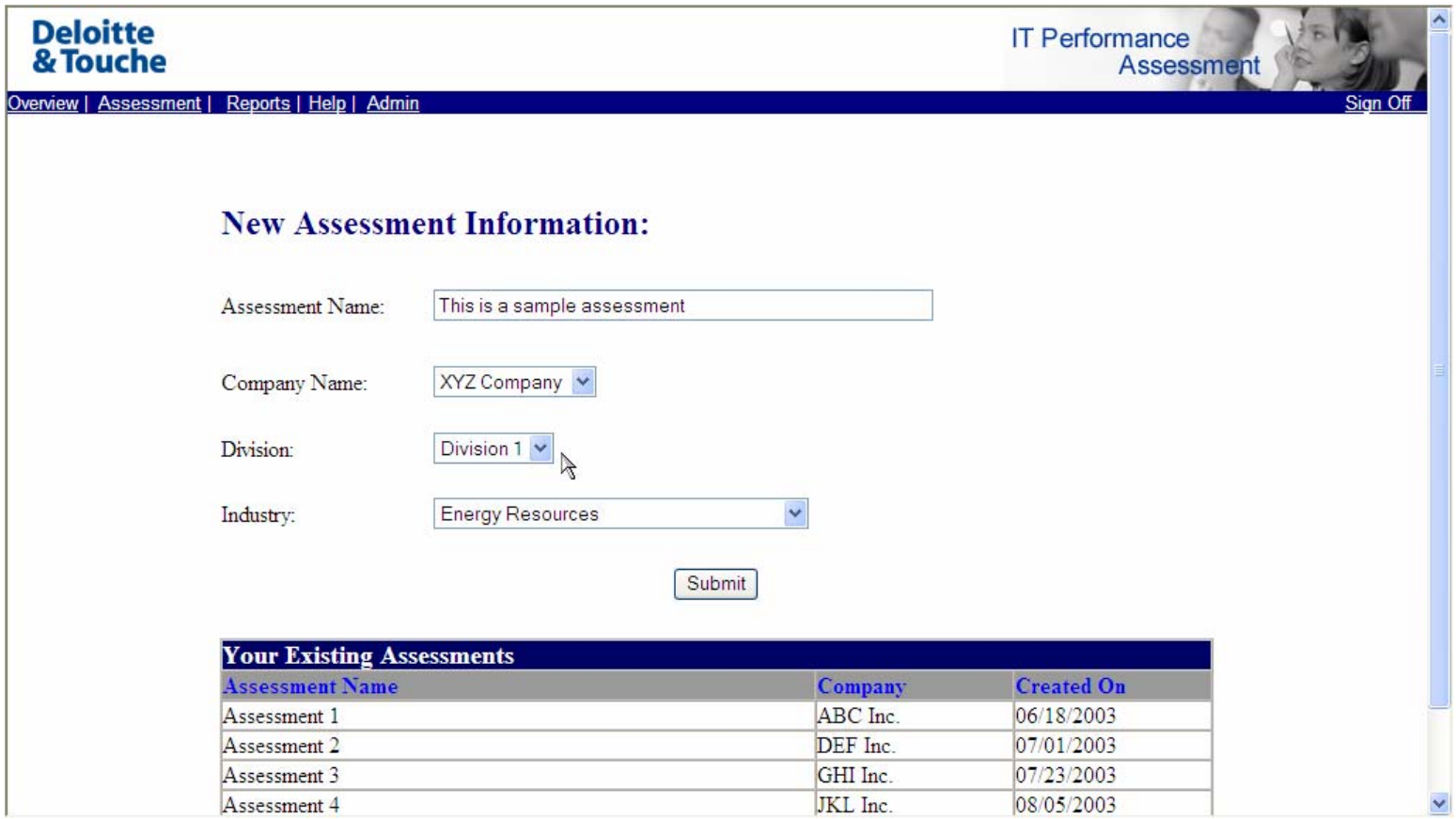
Define Audit Plan

- Priority
  - Results from Risk Assessment
  - Board & Management Requests
- Budget
  - Individual Audit Budgets
  - Total Hours Available
  - Specialists Required
  - Departmental Skill Sets
- Timing
  - Implementation Dates

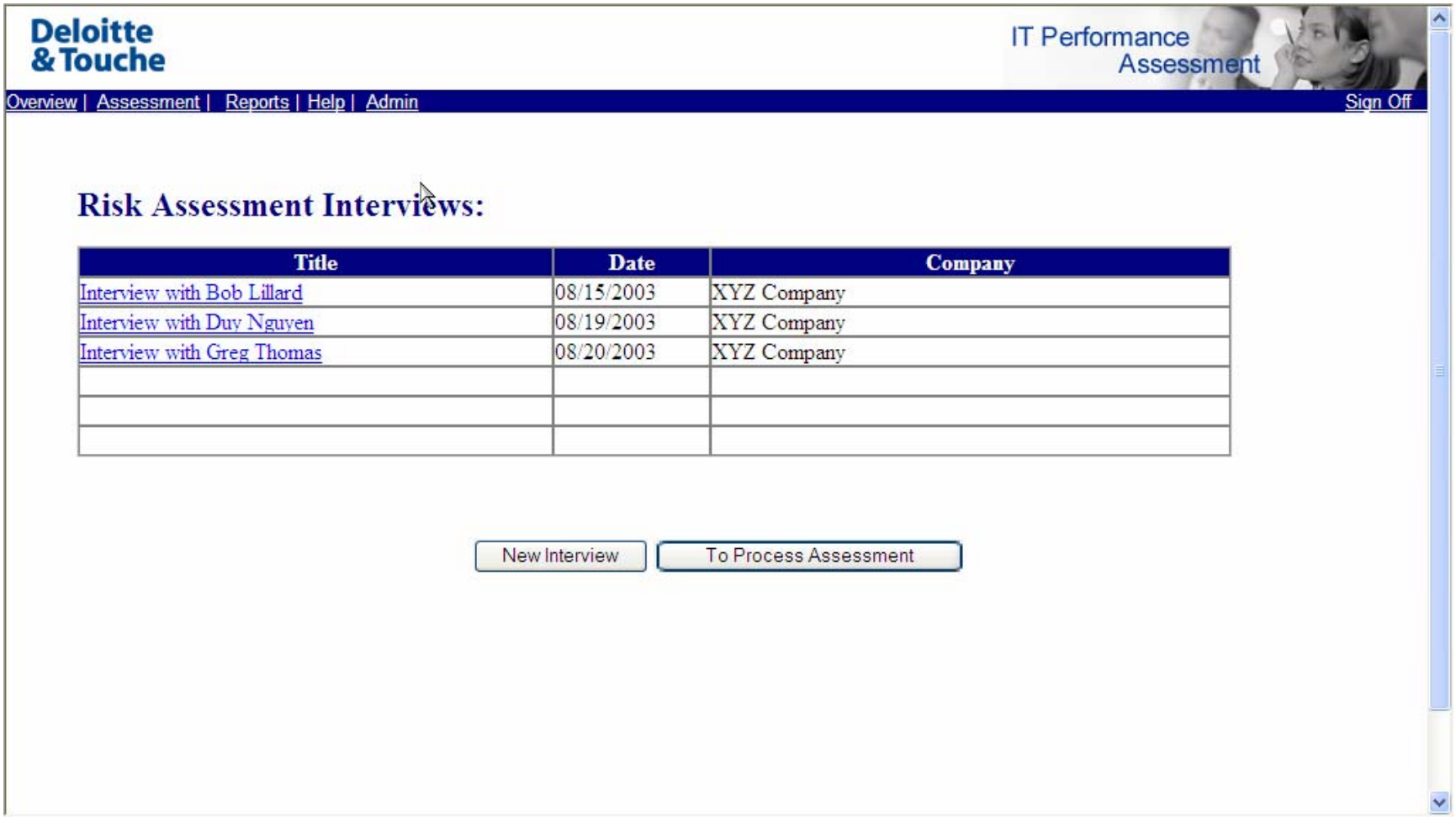
Develop Individual Audit Plans

- 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

IT Assessment Tool



Deloitte & Touche



Deloitte
& Touche

Risk Assessment Input Screen:

Company: Company Name Here

Division: Division Name Here

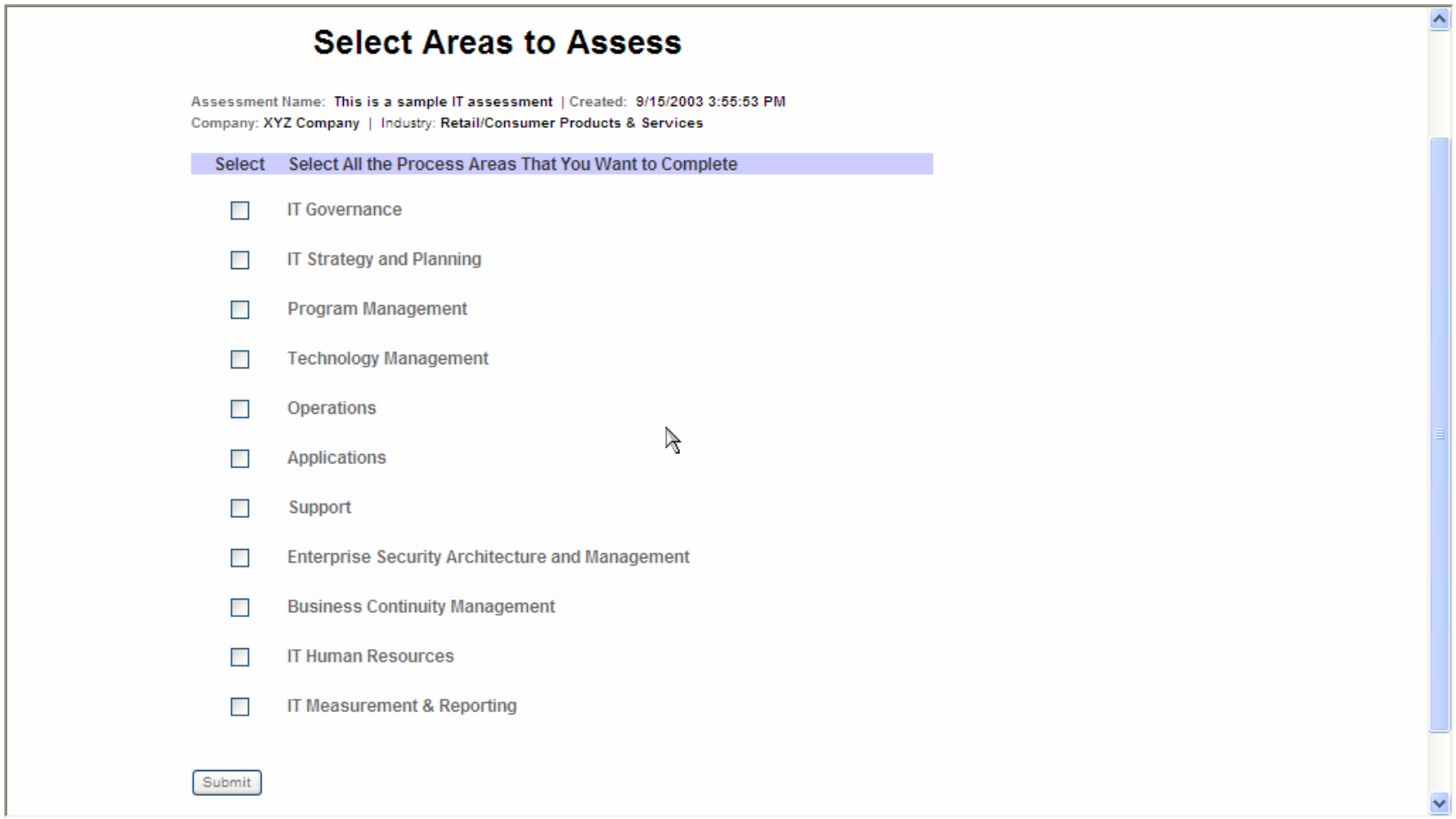
Date: 12/1/2003

Interviewee: Bob Smith

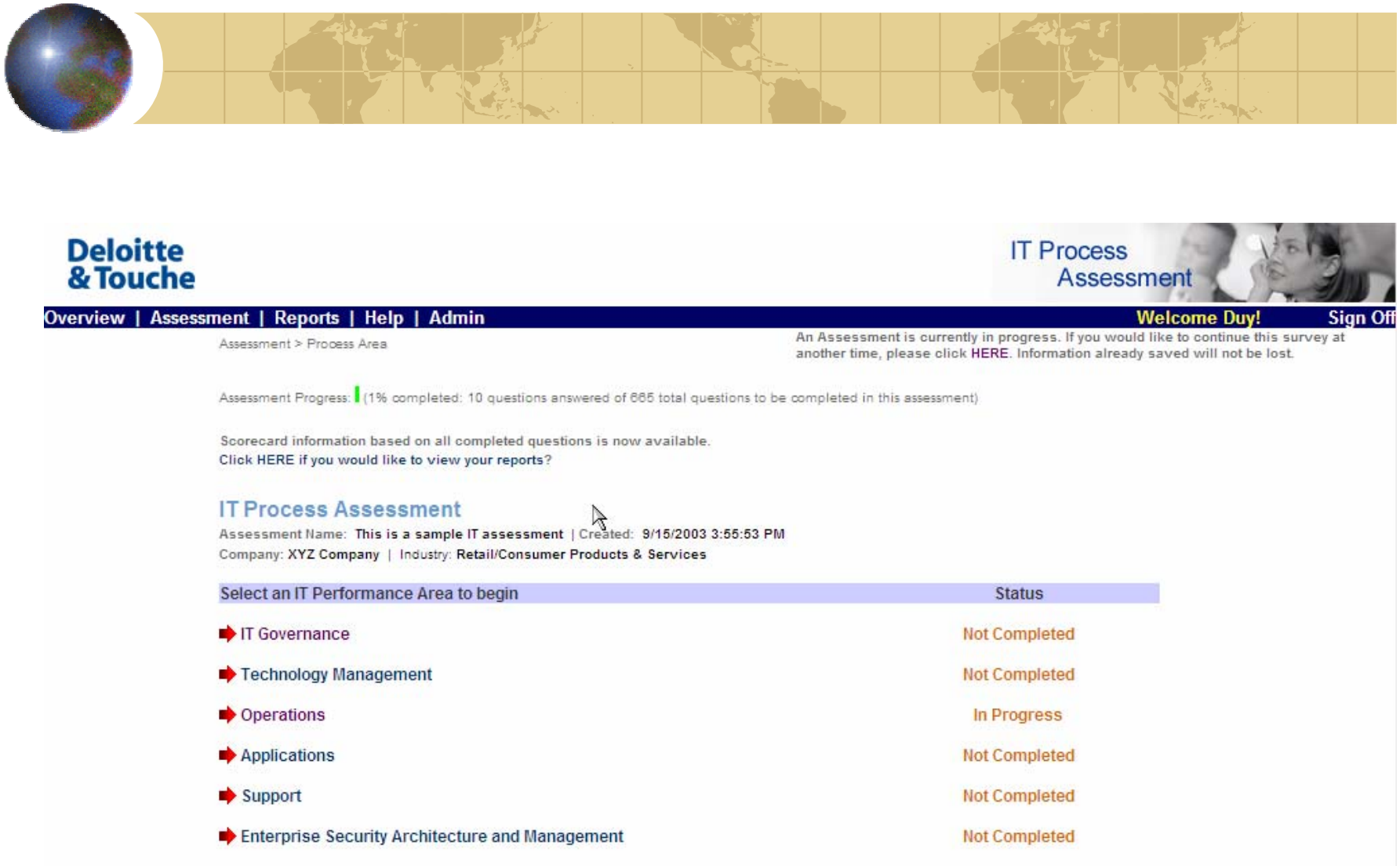
Title: CIO XYZ Company

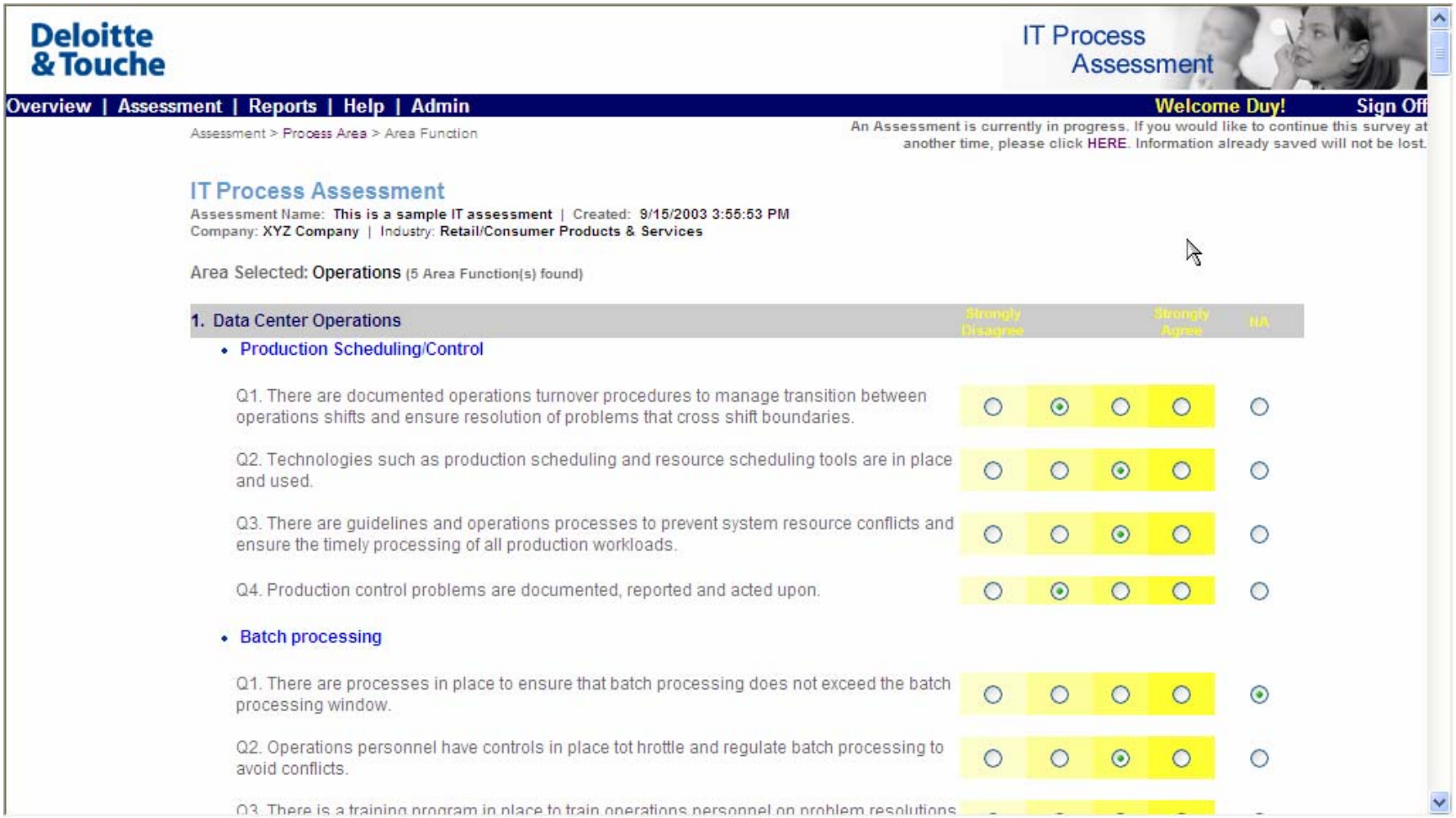
Enterprise IT Risk Areas	Risk		Comments
	H M L n/a		
IT Governance	○ ◉ ○ ○		
IT Strategy & Planning	○ ○ ○ ◉		
Program Management	○ ○ ○ ◉		
Technology Management	○ ○ ○ ◉		
Enterprise Security	○ ○ ○ ◉		
Disaster Recovery	○ ○ ○ ◉		
IT Human Resources	○ ○ ○ ◉		

IT Infrastructure & Application Areas	Mainframe Risk	Mid-Range Risk	Network Risk	Comments
	H M L n/a	H M L n/a	H M L n/a	
IT Operations	○ ○ ○ ◉	○ ○ ○ ◉	○ ○ ○ ◉	

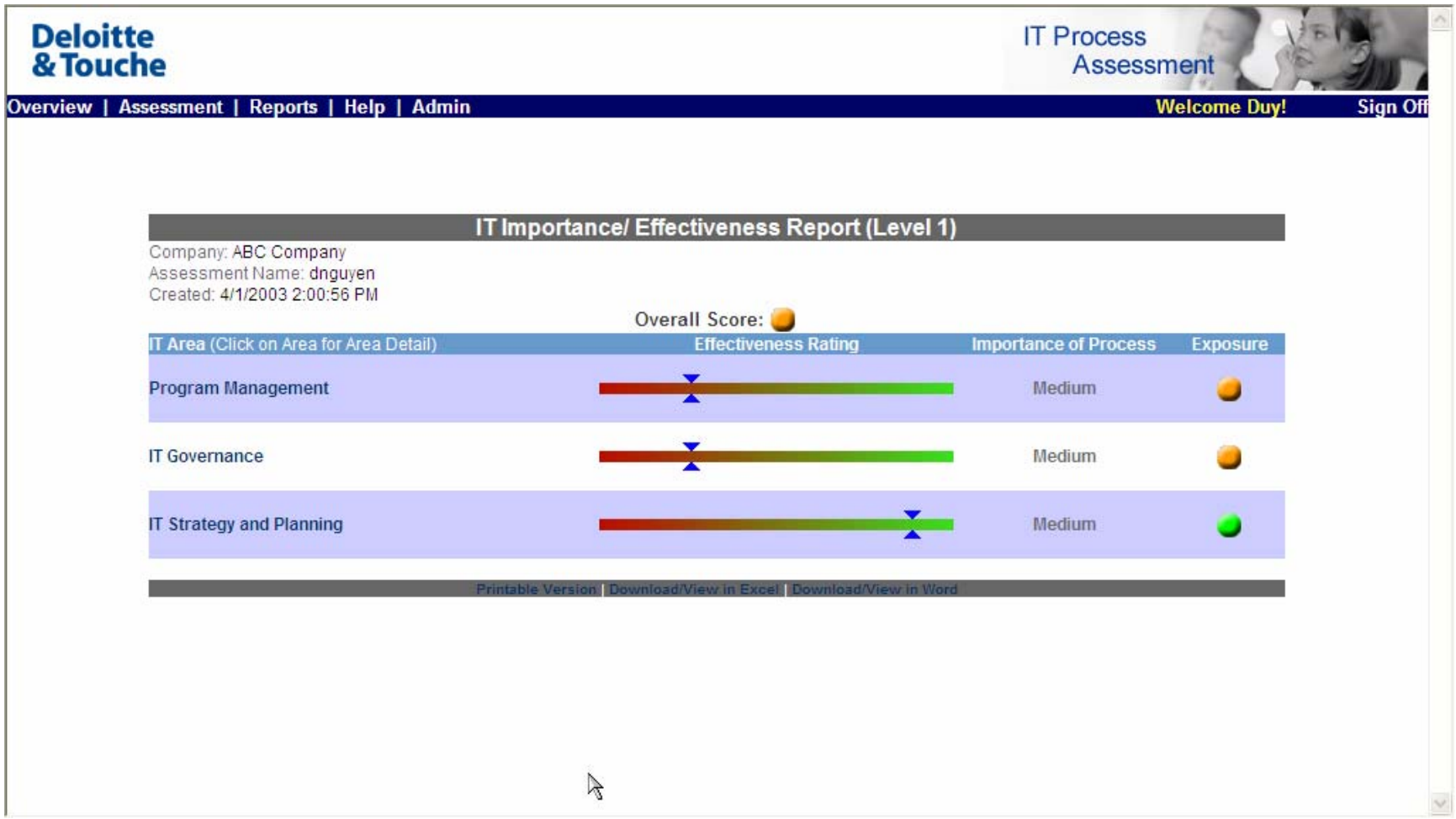


Deloitte & Touche

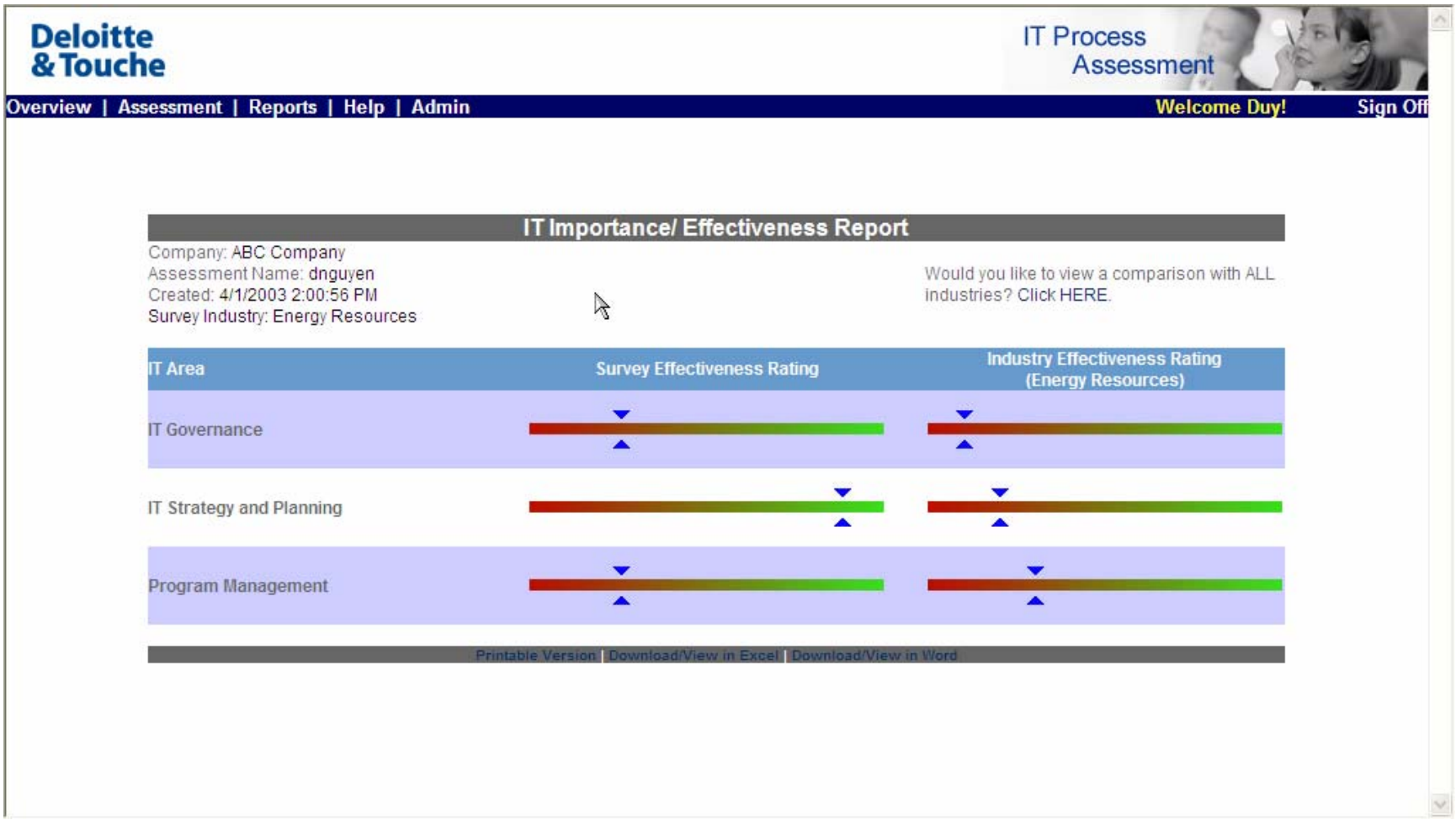

Deloitte & Touche
IT Process Assessment
Overview | Assessment | Reports | Help | Admin
Welcome Duy!
Sign Off
Assessment > Process Area
An Assessment is currently in progress. If you would like to continue this survey at another time, please click HERE. Information already saved will not be lost.
Assessment Progress: (1% completed: 10 questions answered of 665 total questions to be completed in this assessment)
Scorecard information based on all completed questions is now available.
Click HERE if you would like to view your reports?
IT Process Assessment
Assessment Name: This is a sample IT assessment | Created: 9/15/2003 3:55:53 PM
Company: XYZ Company | Industry: Retail/Consumer Products & Services
Select an IT Performance Area to begin
Status
IT Governance
Not Completed
Technology Management
Not Completed
Operations
In Progress
Applications
Not Completed
Support
Not Completed
Enterprise Security Architecture and Management
Not Completed



Deloitte & Touche



Deloitte & Touche



Deloitte & Touche

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