Managing Business Partner Risks

2007 Nebraska Cert Conference

August 14, 2007

About the presenter

Jeff Schreiner, CISSP

- President Continuum Worldwide
- 10 year of information security management
- International business partner risk management experience

Agenda

- Business Partner background
- Trends in Business Partner Risk Management
- Risk Management Lifecycle
- Risk Management Process
- Case Study
- Questions

Business Partner Purpose

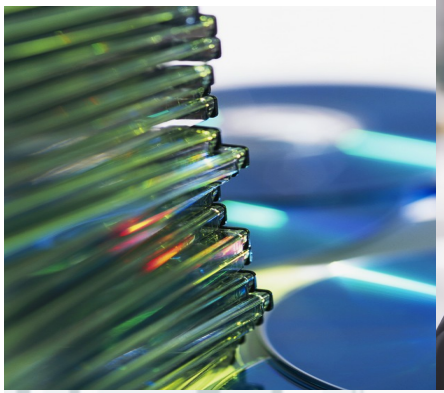
- Business Partners provide the ability for:
  - Business process efficiencies
  - Competitive advantages
  - Cost savings
  - High quality services
- While entrusting:
  - Client/Customer Information
  - Employee information
  - Proprietary information

Business Partner Growth in Business Technology

Global Environment

Why do we care?

- Information
  - Type
  - Classification
- Responsibility
  - Employees
  - Customers
  - Shareholders
- Public Image
  - Brand reputation
  - “Headline avoidance”



Business Partner Growth on a Global Scale

- More than 75 percent of businesses are using outsourced services providers to perform vital business functions
- Global outsourcing industry was the strongest in 1Q'06 with $22.7 billion contracts - *Gartner Research*
- Indian IT Software And Services Grow By 31.4% In FY 05-06 Posting An Aggregate Revenue Of $29.6 Billion *(Source: NASSCOM)*

Business Partner Growth

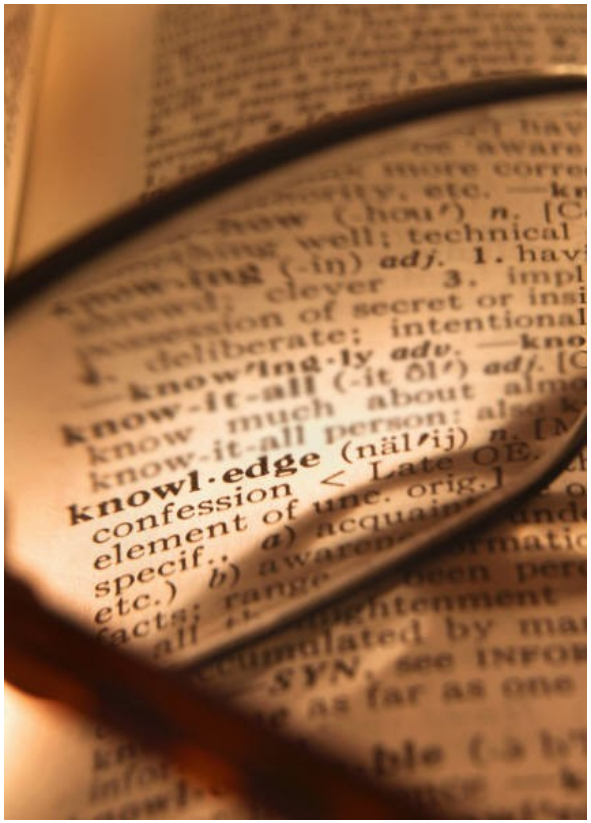
- Why?
  - Outsourcing integration can be done with “ease”
- Management sees outsourcing as:
  - Cost effective
  - Ability to provide service extensibility
  - Focus on core business activities

Business Partner Growth: How does this affect me?

- Growth in business partners access to company information leads to:
  - More responsibility to ensure the protection of company and customer information
  - A drive for more involvement in the management of the business partner relationship
- The challenges facing risk management organizations are:
  - Integrate and develop a risk management program for addressing business partner risk
  - International business partners
  - Managing these risks with a limited amount of resources

Preparing for Business Partner Risk Management: The Drivers

- What are the reasons this relationship is in place?
  - Cost
  - Efficiencies
  - Risk reduction
- Understanding the “Why” will help define controls



Knowledge is key to risk management!

Preparing for Business Partner Risk Management: The Impact

- Understand the impact of a security incident
  - What is affected?
  - Who is affected?
  - How are they affected?

Preparing for Business Partner Risk Management: Culture

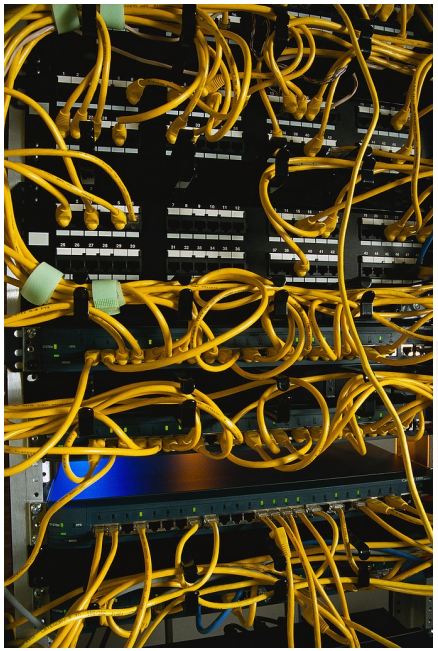
- Business culture of the business partners
  - Similarities
  - Differences
- Geopolitical
  - Global business partner relationships

Preparing for Business Partner Risk Management: Communication

- Person-to-person
  - Relationship managers
  - Stakeholders
  - Avoid Stockholm Syndrome
- Technical
  - Connections between businesses
  - Software
  - Equipment

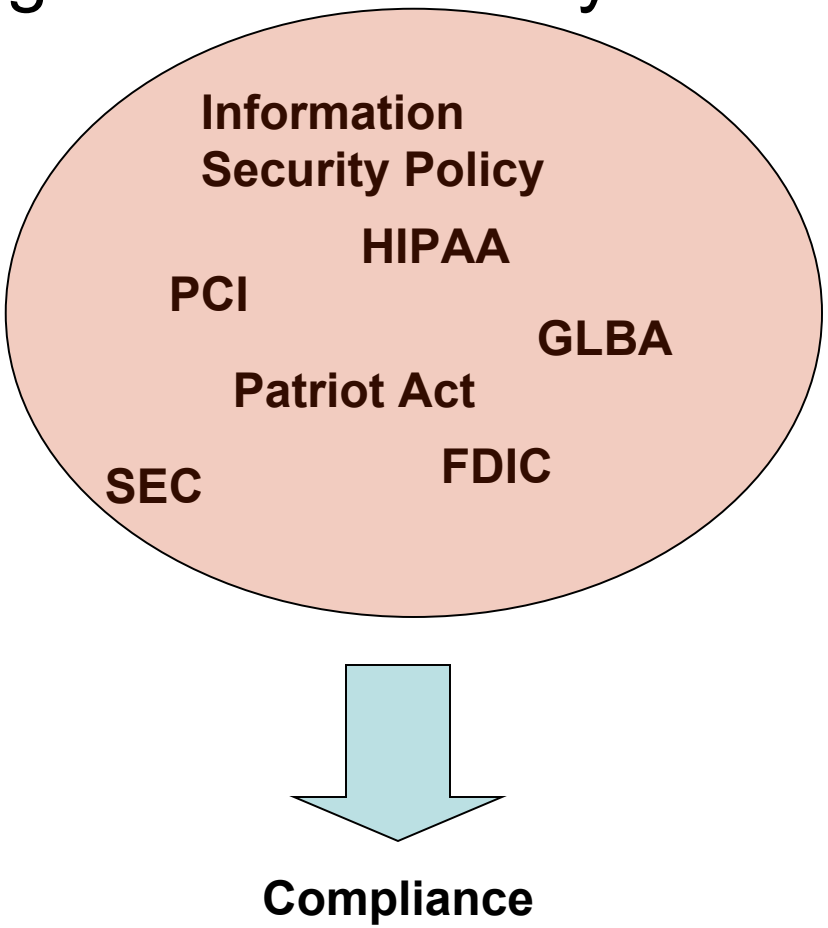
Preparing for Business Partner Risk Management: Communication

- Technical connectivity
  - Direct line
  - MPLS
  - VPN
  - Citrix
- Network access
  - Remote desktop
  - User management
- Monitoring
  - Log review



Preparing for Business Partner Risk Management: Regulations

- Knowing what are the regulations that may govern the relationship
  - Company policy
  - Industry standards
  - Government regulations
- Build them into the controls



Business Partner Risk Management: Due Diligence

- Due diligence is a key element towards managing business partner risk
  - The sooner the better
  - Methods include:
    - **Questionnaires**
    - **Documentation reviews**
    - **On-Site Visits**

Business Partner Risk Management: Due Diligence

- Where is a starting point?
  - Questionnaires
    - **Business Process Owner**
      - **The nature of the relationship**
      - **Type and amount of information**
    - **Business Partner**
      - **Ask how information is protected**
        - » **Physically and Technically**
      - **Based on industry standard (i.e. PCI, NIST, ISO27001)**

Business Partner Risk Management: Due Diligence

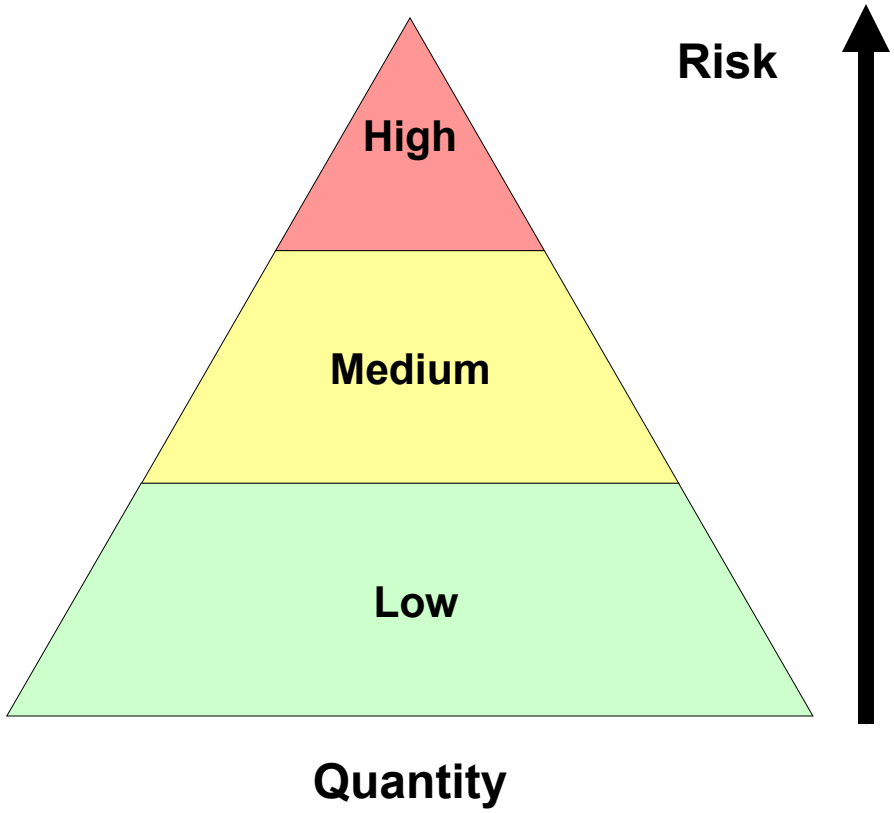
- Where is a starting point?
  - Documentation review
    - **Review all documentation relative to the relationship**
      - **Contract**
      - **Performance Objectives**
      - **Business Partner insurance coverage**
      - **Organizational policies (i.e.)**
        - » **Information Security**
        - » **Human Resources**
        - » **Facilities**

Business Partner Risk Management: Due Diligence

- Where is a starting point?
  - On-Site Visit
    - **Review all documentation *and* physically walkthrough the site**
      - **Work area walkthrough**
      - **Data center tour**
      - **Face to face interviews w/ key personnel**

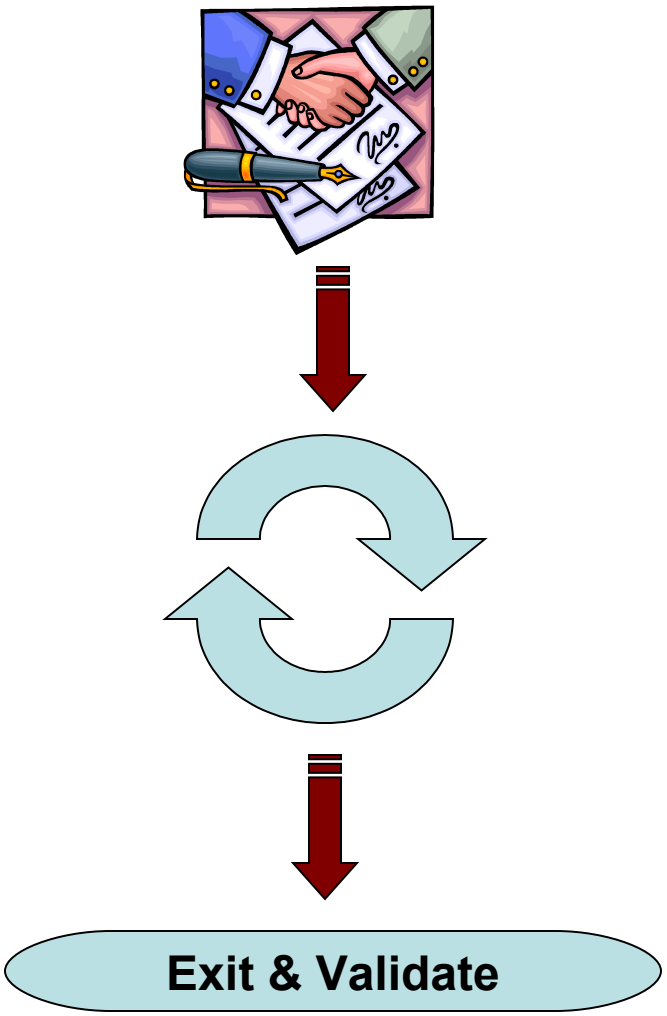
Business Partner Risk Profile

- As risk increases, so do the complexities surrounding the Business Partner relationship
  - Volume
  - Information
- Continuous Assessment may not change the risk profile, but the risk are identified

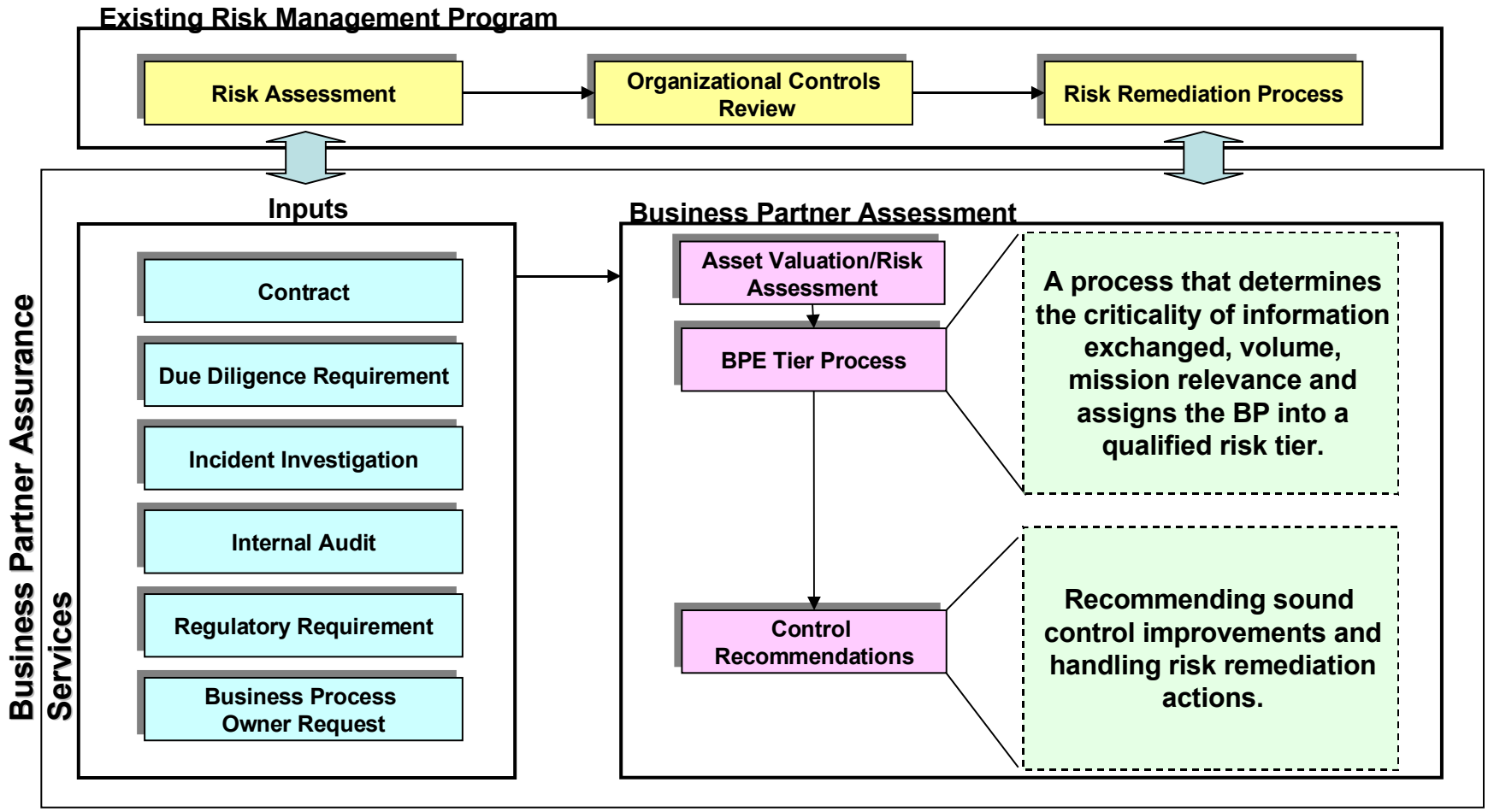


Business Partner Risk Management Lifecycle

- Beginning
  - Due diligence
  - Right to audit
  - Create exit strategy
- Middle
  - Risk Assessment
  - Mitigation
  - Monitoring
- End
  - Execute exit strategy
  - Validation

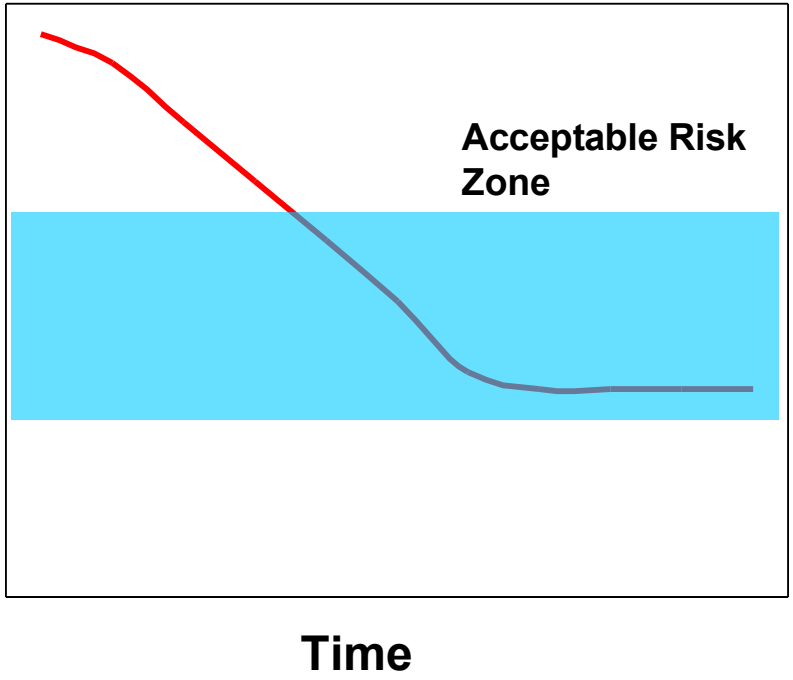


Business Partner Risk Management Lifecycle



Business Partner Assessment Results

- Initial “High” risk business partners may move down in risk
- The goal is to manage the risk with in an acceptable area based on tolerance



Business Partner Risk Management Program Metrics

- Program effectiveness can be tracked by:
  - Review/Assessment cycle frequency
  - Number of business partners reviewed
  - Refining scoring and weighting criteria for questionnaires
  - Incidents that have occurred as a result of the relationship
  - Security awareness surveys to business partner relationship managers

Business Partner Risk Management: Case Study

- Profile: East coast bank
  - 675 branches
  - Provides retail services to individuals and small to medium sized companies
  - Yearly revenue average of $3.2 billion
  - 13,000 employees

Business Partner Risk Management: Case Study

- Drivers
  - FFIEC regulations regarding service provider risk management
  - Concern over business partners that had customer data
  - Internal studies determined a security breach of customer data would cost on average $1 Million

Business Partner Risk Management: Case Study

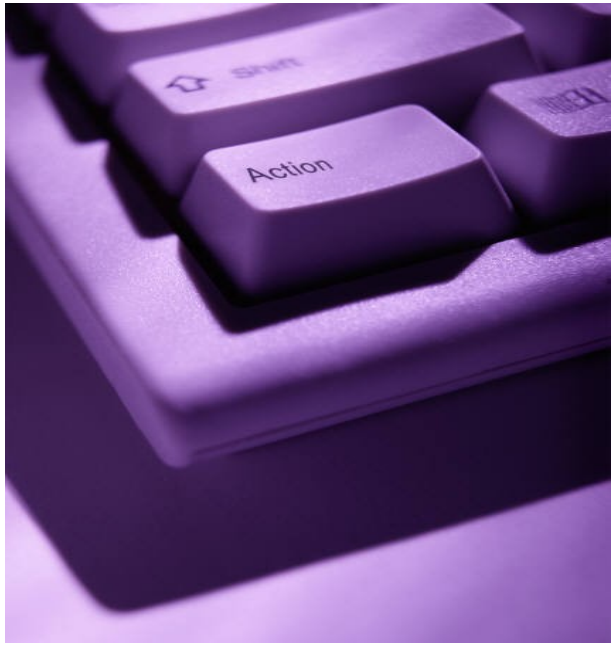
- Business partner profile
  - Over 400 business partners that placed sensitive data at risk
- Problem
  - Business line communication
  - Not enough resources to perform business partner risk management

Business Partner Risk Management: Case Study

- Resolutions
  - Business process ownership identification
    - **Business unit management**
    - **Legal**
    - **Procurement**
    - **Accounts Payable**
    - **Goal: Identify those areas with the business partner relationships**
  - Business process owner questionnaires
    - **Type of data**
    - **Volume**
    - **Goal: Identify the importance and risk associated with the business process and business partner**

Business Partner Risk Management: Case Study

- Resolutions
  - Stream-Line Due Diligence and Risk Rating
    - **Contracted consulting firm**
    - **Developed automated questionnaires and risk rating formulas**
    - **Developed defined action plans**
    - **Implemented continuous monitoring**



Business Partner Risk Management: Case Study

- Results
  - Identified “non-compliant” business units
    - **Increased communication with business unit leadership and associated business partners**
  - Benchmarking Performance
    - **Identify overall due diligence efforts**
    - **Risky business partners**
    - **Focus attention on specific business processes and partners**
    - **Track performance of the compliance and risk management teams**