# Audit Capabilities: Beyond the Checklist

Niall Haddow, Business Leader

Philip Young, Sr. IT Auditor

Professional Strategies - Session S32

# Agenda

- Beyond the Checklist
- Visa Overview
- Visa Internal Audit Overview
- Data Analytics Integration
- Project Reviews & Consultations
- Topical Audit Plan Additions
- Dedicated Forensics Function
- Training/Consultation
- Audit Staffing

# Beyond the Checklist

- Evolving role of Internal Audit
  - The role of IA departments is evolving in response to increasing and broader expectations of audit committees, senior management, and regulators
  - "Leading internal audit functions have aligned themselves with rising stakeholder expectations by expanding the footprint of risks they cover and clearly communicating deeper insights"
    (PwC's 2012 State of the Internal Audit Profession study)

# Visa Overview

- World's Largest Retail Electronic Payments Network
- Visa does not issue cards, extend credit or set rates and fees for consumers.
- Headquartered in San Francisco, Visa's operating regions include:
  - Americas: USA and Canada (NA) / Latin America & Caribbean (LAC)
  - International: Asia-Pacific (AP) / Central and Eastern Europe, Middle East and Africa (CEMEA)
- Visa Europe is a separate entity that is an exclusive licensee of Visa's trademarks.
- Visa became a public company in late 2007, and completed the largest IPO in US history in March 2008.

# Visa Overview

| Statistical Overview* | |
|---|---|
| Financial Institution Clients | 15,000 |
| Visa cards (at 3/31/2012) | 2.0 billion |
| Total Volume (incl. cash) | $6.3 trillion |
| Payments Volume | $3.9 trillion |
| Total transactions | 80 billion |
| ATMs (at 3/31/2012) | 1.96 million |
| Number of employees | 8,000 |

* Data for four quarters ended June 30, 2012
Source: http://corporate.visa.com/_media/visa-corporate-overview.pdf

# Visa Internal Audit Organization

- Prior to becoming a public company in March 2008, Visa internal audit was conducted by separate teams. Since then, Audit has:
  - Consolidated these separate groups into an integrated global department
  - Significantly reduced dependency on external resourcing
  - Implemented new audit methodology and work paper platform
  - Migrated SOX PMO to Finance
  - Developed robust risk assessment program

# Visa Internal Audit Organization

| | |
|---|---|
| Statistical Overview | As of June 30, 2012 |
| Approved FTE | 2009: 32<br>2010-2012: 47 |
| Co-Sourced Resources | 2009: 30-40%<br>2010-2012: 10-20% |
| IT Resources | Represents 45% of IA Staff |
| Major Areas of Audit Emphasis | • Network and Data Security and Privacy<br>• Authorization, Clearing and Settlement<br>• IT Operating Environment<br>• Financial Operations<br>• Regulatory and Policy Compliance<br>• International Operations |

# Visa Internal Audit Organization

- Standard Audit Practices
  - Rotational Risk Based Plan
  - IT & Business Operations Focused Teams
  - Formal Rated Audit Reports & Issue Closure Process
  - Regular Regulatory & External Audit Partner Interactions

# Visa Internal Audit Organization

- Enhanced IA Practices: Beyond the Checklist
  - Data Analytics Integration
  - Project Reviews & Consultations
  - Topical Audit Plan Additions
  - Dedicated Forensics Function
  - Highly Targeted Technical Training & Consultation Approach
  - Audit Staffing

# Data Analytics Integration

# Data Analytics Integration

- FY09 - FY10
  - Ad-hoc data analytics
  - Staff trained on analytic tools (i.e. Excel/Access)
  - Staff performing own data analysis
  - No centralized function to consolidate and automate audit analytics
- FY11
  - Hired data analysis Subject Matter Expert (SME)
  - Provide immediate support on high risk audits

# Data Analytics Integration

- FY11 (con't)
  - Automate and streamline data acquisition
  - Develop and execute data analytics
  - Provide support/guidance for audit staff
- FY12
  - Hired additional SME
  - Detailed ADAP training sessions for IA
  - Developed risk models
  - Built Pipeline for audit assistance

# Data Analytics Integration

- Audit Execution:
  - Planning:
    - Used to identify
      - Areas of higher risk / specific focus
      - Trends and statistics
    - Assistance with budgeting
  - Fieldwork:
    - Test 100% of populations, where possible
    - Provide ad-hoc support/data requests
    - Data validation / simulations

# Data Analytics Integration

- Enhanced Risk Models allow for the identification and risk stratification of areas, including:
  - Vendors
  - Applications
  - Countries
  - Projects
- Outputs of these risk models identify areas of focus for upcoming audits or ad-hoc IA reviews

# Project Reviews & Consultations

# Project Reviews & Consultations

- IA Initiated Push Approach
  - Allows for early advice to management on risk and control considerations so management can develop and proactively implement controls
  - Using data from Visa's project database, augmented by day-today client interactions, IA identifies high-risk projects for review
  - To allow for flexibility and broad coverage, four different approaches are used depending on project risk:
    - Targeted Review
    - On-Going  Monitoring Type I
    - On-Going  Monitoring Type II
    - In-Audit Review
  - Project reviews do not always follow a standard assurance framework in that they do not always require detailed testing and results are not always communicated through an audit report
- Technology Initiated Pull Approach
  - Self-nominated by the Technology organization, who request IA input on specific areas within the project scope

# Topical Audit Plan Additions

# Topical Audit Plan Additions

- Topical / Theme Audit
  - Emerging industry IT risk areas
  - Approach
  - Deliverable
- Current Topical Examples:
  - Social Media
  - Server Virtualization
  - Cloud
  - Cyber Security

# Topical Audit – Social Media

- Why:
  - Rush for Corporate social media presence
  - Increase in public exposure
  - Permanency of social content
- Risks:
  - Data leakage
  - Negative brand impact

# Topical Audit – Social Media

- Scope Areas:
  - Governance
    - Policies & Procedures
    - Risk Assessments
    - Strategy
    - User Training
  - Brand Protection & Business Use of Social Media
    - Corporate Use of Social Media
    - Employee Use of Social Media
    - External User Monitoring
  - IT Security Considerations
    - Access Management
    - Infrastructure Protection

# Topical Audit - Cloud

- Why:
  - Push from market to move to “Cloud”
  - Separate marketing from fact
  - Current and future “Cloud” use
- Risks:
  - Bypass standard purchasing controls
  - Data leakage
  - Security/Reliability relies on Vendor

# Topical Audit - Cloud

- Scope Areas:
  - Definition & Identification
    - Definition
    - Inventory
  - Strategy
    - Cloud use/adoption
  - Technology Oversight & Framework
    - Cloud Acceptable Use
    - Legal & Regulatory Requirements & Compliance
    - Continuous Oversight

# Topical Audit – Server Virtualization

- Why:
  - Cost saving drive virtualization use
  - Growth in ‘Private Cloud’ technologies
  - Expanded use of virtualization in production
- Risks:
  - Hypervisor Creates New Attack Surface
  - More Than One Function per Physical System
  - Mixing VMs of Different Trust Levels
  - Lack of Separation of Duties
  - Information Leakage between Virtual Components

# Topical Audit – Server Virtualization

- Scope Areas:
  - Governance
    - Technology Assessment & Standards
    - Inventory
    - Architecture
  - System Maintenance
    - System Provisioning & Decommissioning
    - Patch Management
  - Access Controls
    - New Users/Obsolete Access
    - Privileged Access

# Topical Audit – Server Virtualization

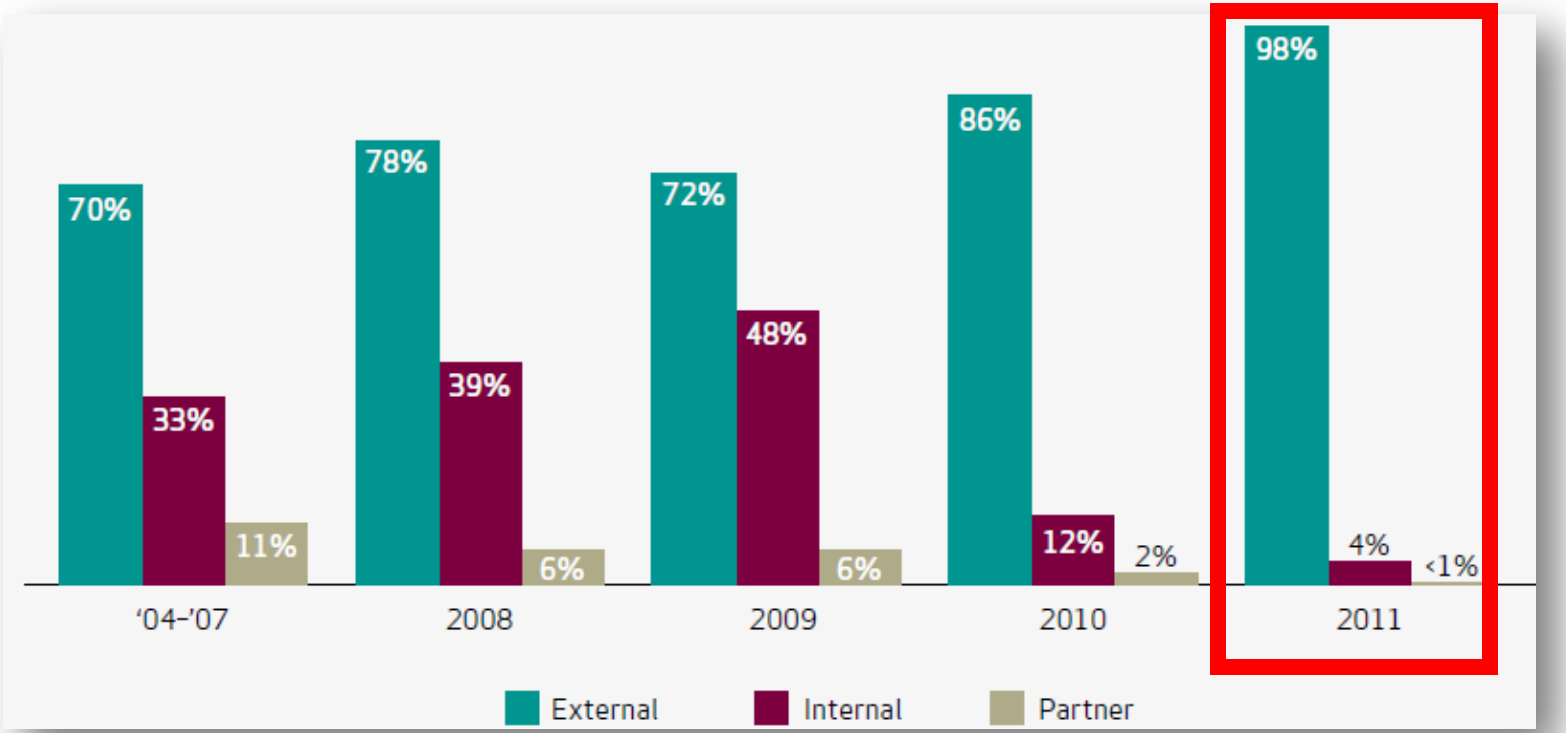
- Scope Areas (Con't):
  - Configuration Management
    - Security Requirements Documented
    - Compliance with Security Requirements
  - Security Assessments & Penetration Testing
    - Vulnerability Scanning
    - Security Assessments

# Topical Audit – Cyber Security

- Why:
  - Increase in number and sophistication of IT security attacks (i.e. APT)
  - Verizon 2012: 855 incidents that were reported in 2011 resulting in 174 million compromised records
- Risks:
  - Loss of Cardholder Data
  - Processing outages
  - Brand reputation
  - Fines

# Topical Audit – Cyber Security

- External threat increase*:




*Verizon Data Breach Investigations Report (DBIR) published in 2012

# Topical Audit – Cyber Security

- Scope Areas:
  - Network Perimeter Security
    - Inventory
    - External Services
    - Configuration
    - External Connections
  - Wireless Security
    - Rogue Access Point
    - Wireless Communication Security
    - Wireless Intrusion Detection

# Topical Audit – Cyber Security

- Scope Areas (con't):
  - Data Loss Prevention & Detection
  - Intrusion Prevention & Detection
    - Prevention and Detection of Malicious Software
    - Prevention and Detection of Prohibited Tools
  - Distributed Denial Of Service (DDoS) Mitigation
    - DDoS Mitigation
    - DDoS Detection and Reporting
  - Social Engineering Prevention
    - Policies and Procedures
    - Training and Awareness

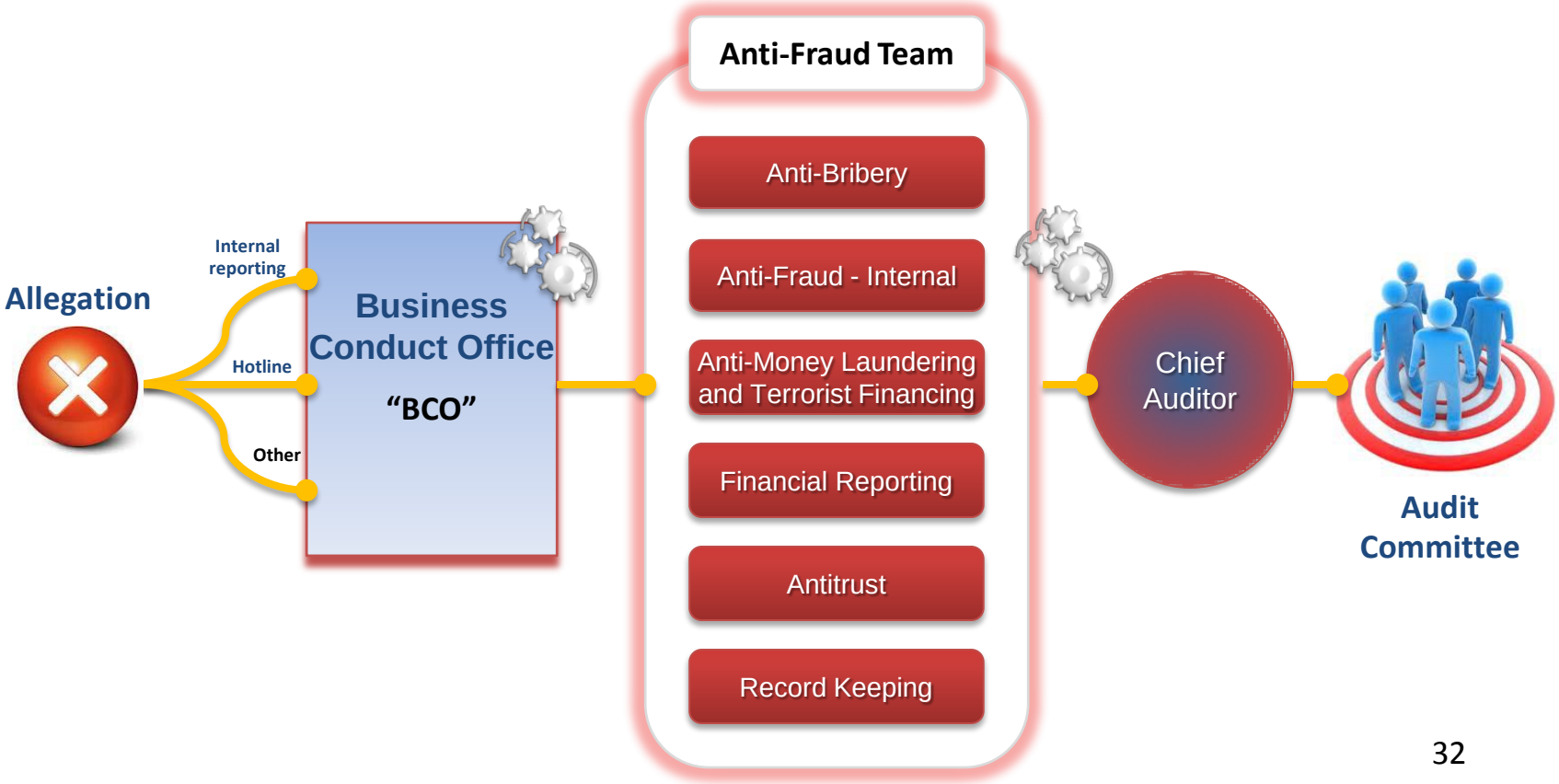
# Dedicated Anti-Fraud Function

# Dedicated Anti-Fraud Function

- Responsible for developing and executing investigative and anti-fraud policies and procedures
- Type of projects:
  - Leading investigations and forensic technology projects
  - Working with the Audit Management Team to enhance the proactive consideration of fraud risks in audits
  - Conducting proactive forensic work including data analysis projects, vendor audits, and other Chief Auditor identified special projects

# Dedicated Anti-Fraud Function

- Investigation Process Flow & Examples



# Dedicated Anti-Fraud Function

- Data Sources & Tools Used

| Electronic Data Sources | Collection and Review Tools |
|---|---|
| Forensic Hard Drive Imaging | Encase, FTK |
| Electronic Data Review | Clearwell |
| Email Exchange Server | ExMerge – Creates .pst file |
| Connected Backup | Classify & Collect |
| Network Group and User Share | RoboCopy – Preserves metadata |
| Instant Messaging | Systems Engineering Team |
| Forensic Imaging of Cell Phones and Other Removable Media | Forensic Imaging of Cell Phones and Other Removable Media |
| Backup Tapes | Various Restoration Tools |
| Voicemail | Various Review Tools |

# Targeted Technical Training & Consultation

# Training/Consultation

- With IT risks constantly evolving, training is a vital step for ensuring continued appropriate audit techniques and control evaluations
- IA training budgets are typically strained, so consider:
  - Approaching HR to talk about Education Assistance Programs
  - Vendor led internal trainings/consultations (e.g. IBM Mainframe training)
- Individuals are encouraged to become Subject Matter Experts:
  - Mobile (Payment/Security)
  - IT Security Trends
  - Disaster Recovery
  - Encryption

# Training/Consultation

- Not only attend but provide!
- Give talks internally:
  - Lunch and Learns
  - 5-15 minute blocks in monthly staff meetings
  - Disseminate information learned at events
    - E.g. 15 minutes about COBIT 5 changes
- Give talks externally at events
  - ISACA
  - IT Security Events

# Training/Consultation

- Audit Topic Specific Trainings:
  - RACF/Mainframe
  - Disaster Recovery Institute (DRI) Certification
  - Ethical Hacking & Hacker Techniques
  - TCP/IP Networking

# Training/Consultation

- Participate in leadership knowledge sharing
  - Silicon Valley IT Audit Director Round Tables
  - PwC West Regional IT Audit Director Round Table
  - ISACA IT Audit Director Round Table

# Training/Consultation

- Consultations:
  - Industry recognized experts brought in as consultants
    - IBM Mainframe Security Consultant
    - Ethical Hacker
    - Deloitte Cloud SME
- Unexpected Challenges

# Audit Staffing

# Audit Staffing

- Integrated Staffing
  - Team cross pollination
  - Staff audit bidding allows for development interests
- Subject Matter Experts
  - Disaster Recovery
  - IT Security
  - Encryption
  - Virtualization

# Questions