IT Audit “Hot Topics”
Social Media, The Cloud, IT Governance, Big Data, and More

Charlotte ISACA Chapter
Annual General Meeting

June 25, 2013
Introductions

- Josh McDermott, CISA, CISSP, PMP
  
  *Director, IT Audit, TIAA-CREF*

- Ben Schmidt, CISA, CISSP
  
  *Lead IT Auditor, TIAA-CREF*
The viewpoints contained within this presentation are those of the individual presenters.

All scenarios are theoretical examples.

Some of the material comes from…. the internet!

(your mileage may vary)
Agenda

• Social Media
• Big Data
• IT Governance
• Mobile Computing and Security
• Data Protection / DLP
• Cloud Computing
• Integrated Auditing
Agenda

• Definition of “Social Media”

• Benefits of Social Media

• Social networking statistics for 2013

• Key risks
Social Media Explained – the donut example

SOCIAL MEDIA EXPLAINED

TWITTER  I'M EATING A #DONUT
FACEBOOK  I LIKE DONUTS
FOURSQUARE THIS IS WHERE I EAT DONUTS
INSTAGRAM  HERE'S A VINTAGE PHOTO OF MY DONUT
YOUTUBE  HERE I AM EATING A DONUT
LINKED IN  MY SKILLS INCLUDE DONUT EATING
PINTEREST  HERE'S A DONUT RECIPE
LAST FM  NOW LISTENING TO "DONUTS"
G+  I'M A GOOGLE EMPLOYEE WHO EATS DONUTS.
The landscape… (what are you auditing / controlling)
ISACA’s view…

“Social media” is defined as using Internet-based applications or broadcast capabilities to disseminate and/or collaborate on information.

– ISACA Social Media Audit Assurance Program
What are the benefits of leveraging Social Media?

Companies are increasingly using Social Media to:

- Improve customer satisfaction and loyalty
- Engage customers in real-time
- Recruit / retain top talent
- Build and enhance brand awareness
- Address any negative publicity or misunderstanding
- Monitor the marketplace

http://blog.microsecommerce.com
Social networking usage statistics for 2013

**Facebook**
1.1 billion monthly active users

**Twitter**
288 million monthly active users

**YouTube**
1 billion unique monthly visitors

**Google+**
359 million monthly active users

**LinkedIn**
Over 200 million users

http://smallbusiness.yahoo.com
## What are the risks?

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic</strong></td>
<td>Unclear, inconsistent, or inaccurate customer messaging</td>
</tr>
<tr>
<td><strong>Data / System Security</strong></td>
<td>Viruses / malware; employee and third-party access through company or private networks</td>
</tr>
<tr>
<td><strong>Loss of Sensitive Information</strong></td>
<td>Disclosure of company information (intentional or unintentional); less control over corporate content</td>
</tr>
<tr>
<td><strong>Reputation</strong></td>
<td>Negative online commentary about company, products, services; hijacking of brand; loss of trust</td>
</tr>
<tr>
<td><strong>Legal / Regulatory Infractions</strong></td>
<td>Loss of personal information about customers or employees; disclosure of non-public information; lack of consumer/privacy disclosures</td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Impact company’s stock price; abnormal customer turnover</td>
</tr>
<tr>
<td><strong>Personal Safety</strong></td>
<td>Information about employee activities/travel</td>
</tr>
<tr>
<td><strong>Data Retention</strong></td>
<td>Records management requirements; e-discovery</td>
</tr>
</tbody>
</table>
- Hacks and breaches continue; corporate social media accounts and customer accounts are at risk.
  - Two step authentication
- Is Social Media really an “IT” issue?
- Increasing regulatory guidance / scrutiny
  - FFIEC proposed guidance (January 2013)
  - FINRA targeted “spot check” (June 2013)
IT Audit Hot Topics: “Big Data”

June 25, 2013
Agenda

• What is Big Data?

• What are the risks? Why does it need to be audited?

• Common Big Data Terminology

• Common Big Data Technology

• References
What is Big Data?

Simply put, it is data sets that—due to their size (Volume), the speed they are created with (Velocity), and the type of information they contain (Variety)—are pushing the existing infrastructure to its limits.

Other “Vs” can also be used to discuss Big Data, such as Variability and Value.

<table>
<thead>
<tr>
<th>Volume</th>
<th>Velocity</th>
<th>Variety</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 90% of the worlds data was created in the last 2 years</td>
<td>• Business Transactions</td>
<td>• Structured</td>
</tr>
<tr>
<td>• 1 EB = 100000000000000000 Bytes</td>
<td>• Security / Fraud</td>
<td>• Semi-structured</td>
</tr>
<tr>
<td>• 2.5 EB’s are created every day</td>
<td>• Marketing</td>
<td>• Semi-unstructured</td>
</tr>
<tr>
<td>• Gigabyte (GB) - 1,024MB</td>
<td>• Customer Relationship Management (CRM)</td>
<td>• Poly-structured</td>
</tr>
<tr>
<td>• Terabyte (TB) - 1,024GB</td>
<td>• Machine / Device</td>
<td>• Unstructured data</td>
</tr>
<tr>
<td>• Petabyte (PB) - 1,024TB</td>
<td>• Social Media</td>
<td></td>
</tr>
<tr>
<td>• Exabyte (EB) - 1,024PB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Mario Bojilov, President, Board of ISACA-Brisbane and Domo.com
### What are the risks? Why does it need to be audited?

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic &amp; Reputation Risk</td>
<td>Design and implementation is not coordinated with / does not meet the needs of the business.</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Excessive time required to analyses and output the required information.</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Unavailability of the data in the event of an unforeseen disaster / disruption.</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Inconsistent data definitions, creating confusion, errors and inefficiencies in the access of data by business users.</td>
</tr>
<tr>
<td>Operational and Accounting Risk</td>
<td>Data integrity is not maintained or is inconsistent with data stored in other areas of the organization.</td>
</tr>
<tr>
<td>Operational Risk</td>
<td>Inaccurate information is inappropriately relied upon for other processing / decision making.</td>
</tr>
<tr>
<td>Operational &amp; Security Risk</td>
<td>Unauthorized / inappropriate access to or editing of data.</td>
</tr>
<tr>
<td>Legal, Compliance, and Security Risk</td>
<td>Data privacy and confidentiality is not maintained</td>
</tr>
</tbody>
</table>

Source: Institute of Internal Auditors (IIA) Audit Executive Center and Open Data Center Alliance: Big Data Consumer Guide
### Common Big Data Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache™ Hadoop®</td>
<td>An open-source storage and processing framework based on MapReduce, using a distributed file system.</td>
</tr>
<tr>
<td>BigTable</td>
<td>A type of NoSQL database that is based on Google's BigTable paper from 2006. In essence, it is a highly scalable, sparse, distributed, consistent multidimensional sorted map.</td>
</tr>
<tr>
<td>distributed file system</td>
<td>A file system that allows access to files from multiple hosts sharing a computer network. Hadoop and other Big Data technologies use this approach to implement parallel processing and improve availability and performance. Distributed file systems often imply replication of data and fault tolerance.</td>
</tr>
<tr>
<td>document store</td>
<td>A type of NoSQL database that stores entire documents.</td>
</tr>
<tr>
<td>graph database</td>
<td>A type of NoSQL database that uses graph structures with nodes, edges, and properties to represent and store data.</td>
</tr>
<tr>
<td>key-value store</td>
<td>A type of NoSQL storage that enables storage of arbitrary data (a value) using a unique identifier (key).</td>
</tr>
<tr>
<td>machine learning</td>
<td>A branch of artificial intelligence concerned with the development of algorithms that take as input empirical data, such as from sensors or databases. The algorithm is designed to identify complex relationships thought to be features of the underlying mechanism that generated the data and employ these identified patterns to make predictions based on new data.</td>
</tr>
<tr>
<td>MapReduce</td>
<td>A programming paradigm that enables parallel processing.</td>
</tr>
<tr>
<td>massively parallel processing (MPP)</td>
<td>The coordination of a large number of processors (or separate computers) to perform computations, where a processor or group of processors works on different parts of the program.</td>
</tr>
<tr>
<td>NewSQL</td>
<td>A category of databases that uses new approaches to modify the underlying architecture of SQL databases so that they can scale similar to many NoSQL technologies.</td>
</tr>
<tr>
<td>NoSQL (not only SQL)</td>
<td>A broad class of non-relational, non-SQL databases that often does not offer ACID guarantees. This class of databases encompasses document store, key-value store, BigTable, and graph databases. This class of databases is useful for working with huge quantities of data—structured or unstructured—when the ability to store and retrieve vast quantities of data is more important than the ability to examine the relationships between the data elements.</td>
</tr>
<tr>
<td>polystructured data</td>
<td>Data that is in various formats, and those formats may change over time.</td>
</tr>
<tr>
<td>streaming analytics</td>
<td>Analysis of data as it is generated—data in motion. To be compared to the analysis of data after persistence—data at rest.</td>
</tr>
<tr>
<td>structured data</td>
<td>Data that resides in fixed fields within a record or file such as a relational database or a spreadsheet.</td>
</tr>
<tr>
<td>unstructured data</td>
<td>Information that either does not have a pre-defined data model or does not fit well into predefined attributes or row/column formats.</td>
</tr>
</tbody>
</table>

Source: Open Data Center Alliance: Big Data Consumer Guide
Common Big Data Technology

Source: Open Data Center Alliance: Big Data Consumer Guide
• ISACA Big data defined (isaca.org)

• IIA Audit Executive Center (cae.theiia.org)

• Open Data Center Alliance: Big Data Consumer Guide
IT Audit Hot Topics: IT Governance

June 25, 2013
Importance of IT governance

What is IT Governance (ISACA)

The leadership and organizational structures and processes that ensure that information technology sustains and extends the organization's strategies and objectives

ISACA Requirement Standard 10 – IT Governance

The IS auditor should review and assess whether the IS function aligns with the organization's mission, vision, values, objectives and strategies.

IIA Requirement – IPPF 2110 Governance

A2: The internal audit activity must assess whether the information technology governance of the organization supports the organization’s strategies and objectives
## Available Guidance

<table>
<thead>
<tr>
<th>COBIT</th>
<th>ISACA</th>
<th>IT Governance Institute (ITGI)</th>
<th>The IIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A business framework for the governance and management of enterprise IT</td>
<td>• IS Auditing Guideline G18, IT Governance</td>
<td>• <a href="http://www.itgi.org">http://www.itgi.org</a></td>
<td>• GTAG 17 Auditing IT Governance (Jul 12)</td>
</tr>
<tr>
<td>• COBIT Online</td>
<td></td>
<td></td>
<td>• Five Governance Components</td>
</tr>
<tr>
<td>• COBIT 4.1 – Monitor and Evaluate 4 (ME4) – Provide IT Governance</td>
<td></td>
<td></td>
<td>o Organization and Governance Structures</td>
</tr>
<tr>
<td>• COBIT 5 (April 2012)</td>
<td></td>
<td></td>
<td>o Executive Leadership and Support</td>
</tr>
<tr>
<td>• Separating governance from management</td>
<td></td>
<td></td>
<td>o Strategic and Operational Planning</td>
</tr>
<tr>
<td>• Direct, Evaluate and Monitor</td>
<td></td>
<td></td>
<td>o Service Delivery and Measurement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o IT Organization and Risk Management</td>
</tr>
</tbody>
</table>
Components of IT Governance (control objectives)

Strategic alignment
• IT strategy aligns with business goals

Value delivery
• Monitoring of IT services
• Balance of risk and benefit

Resource management
• High level direction for sourcing and use of resources
• Optimal balance between sustaining and growing the enterprise

Risk management
• Board awareness of IT risk exposures

Performance measurement
• IT scorecard linked to business goals
Potential Pitfalls/Challenges

Politically difficult audit

– Audit may strain relationship with senior IT leadership.
– Perception of “going after” the CIO
– Ineffective IT governance may be indicative of poor oversight by the CEO, senior management or the Board.

Management may simply complain about IT

• Frustration over delivery, service and support issues. “Noise”

Debate over root cause

• Ineffective IT governance, unrealistic demands from business, or inadequate funding
IT Audit Hot Topics: Mobile Computing and Security

June 25, 2013
Agenda

• Mobile Computing in the Business
• Risks of Mobile Computing
• Mobile Security
• Mobile Security Management
• References
Mobile Computing in the Business

Dramatic shift in the role of mobile devices.

Past
- Devices were locked down by IT department
- Deployed and managed with little to no input from end users or business managers
- Minimal access to business information

Shift
- Variety of device models and types
- Devices chosen by employee or business managers
- Access to more business information from any location.

<http://www.dimensionalresearch.com/>
The business risks include:

- Information interception resulting in a breach of sensitive data, enterprise reputation, adherence to regulation and legal action
- Malware propagation, which may result in data leakage, data corruption and unavailability of necessary data
- Device corruption, lost data, call interception and possible exposure of sensitive information
- Lost devices or unauthorized access to unsecured devices allowing exposure of sensitive data, resulting in damage to the enterprise, customers or employees
- Data leakage, malware propagation and unknown data loss in the case of device loss or theft
Mobile Security

Device security policies

Inherent device security – encryption, authentication, malware protection

Protected access to business – VPN, encrypted networks

Best Practices

Prohibit the use of custom ROMs (i.e. jail breaking) and unauthorized App markets or sites

Regularly scan mobile devices with anti-virus and anti-malware

Protect and backup information on the devices

Wipe and lock stolen and lost devices as soon as being notified by employees
• ISACA Mobile Computing Security Audit / Assurance Program

IT Audit Hot Topics: Data Protection
/Data Loss Prevention

June 25, 2013
Agenda

• What is Data Protection / Data Loss Prevention (DLP)?

• What Are Some Risks Associated with Data?

• Controls to Help Mitigate the Risks
Data Protection / Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself.

Source: http://www.sans.org/critical-security-controls
## What Are Some Risks Associated with Data?

<table>
<thead>
<tr>
<th>Risk of Theft</th>
<th>Deliberate attacks on systems and individuals who have access to sensitive data can cause more harm than inadvertent exposure. Former employees, inside people who have a grudge against an organization, or criminals looking to make money from the sale of the data will look for data stored on laptops, hard drives, and thumb drives. Insiders are the number one cause of data breaches, while hackers rank a bit lower, according to one study by the Ponemon Institute.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk of Loss</td>
<td>Inadvertent exposure due to the loss of media is another way data is exposed. Backup tapes or paper files being misplaced on their way to a storage facility, or laptops left behind at airports or in taxis, are common ways data can end up in the hands of unauthorized people.</td>
</tr>
<tr>
<td>Risk of Neglect</td>
<td>When old computers or hard drives are sold or recycled, the information contained on them might be deleted, but if not properly erased, that data can be retrieved by anyone with just a few cheap tools. Additionally, leaving data on media that is not adequately protected with a strong password or with encryption leaves it vulnerable to a hacker or thief.</td>
</tr>
<tr>
<td>Risk of Insecure Practices</td>
<td>Collecting, storing, sending, encrypting, finding and removing data may all have implications for its safety. Those who are handling sensitive data, may find they are doing one or more of these activities. If proper safety precautions are not taken, inadvertent data exposure could be the result.</td>
</tr>
</tbody>
</table>
Controls to Help Mitigate the Risks

Step 1: Data encryption system ensures that appropriate hard disks are encrypted
Step 2: Sensitive network traffic encrypted
Step 3: Data connections monitored at the network’s perimeter by monitoring systems
Step 4: Stored data scanned to identify where sensitive information is stored
Step 5: Offline media encrypted

Source: http://www.sans.org/critical-security-controls/control.php?id=17
IT Audit Hot Topics: Cloud Computing

June 25, 2013
Agenda

• What is Cloud Computing?

• Cloud Computing Benefits

• Cloud Computing Challenges

• References
What is Cloud Computing?

The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Source: NIST
The NIST Cloud Definition Framework

- **Hybrid Clouds**
  - **Private Cloud**
  - **Community Cloud**
  - **Public Cloud**

**Deployment Models**
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

**Service Models**
- On Demand Self-Service
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service

**Essential Characteristics**
- Massive Scale
- Homogeneity
- Virtualization
- Low Cost Software

**Common Characteristics**
- Resilient Computing
- Geographic Distribution
- Service Orientation
- Advanced Security

Source: NIST
Cloud Computing Benefits

- Rapid deployment of applications and resources
- Available anywhere and anytime
- Cost savings due to reduction of capital expenditures and IT staff
- Operating expenses (vs. Capex)
- Reduce power consumption (aka: Green savings)
- Scalable
- Maintenance and availability become someone else’s responsibility
- No more buying servers (Under-utilization and rapid depreciation)
- No buying switches, routers, cabling, backup power, redundant bandwidth, and HVAC
- Reduce IT staff for server maintenance and server/computer rooms.
- They buy equipment, you rent (By the gigahertz, gigabyte, kilowatt, Mbps)
- They hire IT staff, you rent their services
- Possible economies of scale. Lower capital expenditures and IT operating costs

Source: NIST
Cloud Computing Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Challenge Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data location</td>
<td>Regardless of the deployment model selected, customers may not know the physical location of the server used to store and process their data and applications.</td>
</tr>
<tr>
<td>Commingled data</td>
<td>Many clients will use the same application on the same server concurrently, which may result in the clients’ data being stored in the same data files.</td>
</tr>
<tr>
<td>Cloud security policy/ procedure transparency</td>
<td>Some CSPs may have less transparency than others when it comes to their current information security policies.</td>
</tr>
<tr>
<td>Cloud data ownership</td>
<td>Contract agreements may state that the CSP owns the data placed in the cloud computing environment that it maintains.</td>
</tr>
<tr>
<td>Lock-in with CSP’s proprietary APIs</td>
<td>As in the 1970s, with proprietary software vendor applications, many CSPs currently implement their applications using proprietary APIs. This makes transitioning between CSPs extremely difficult, time-consuming and labor-intensive.</td>
</tr>
<tr>
<td>CSP business viability</td>
<td>As cloud computing continues to mature, there will be CSPs going out of business.</td>
</tr>
<tr>
<td>Record protection for forensic audits</td>
<td>Clients must also consider the availability of data and records if required for forensic audits.</td>
</tr>
<tr>
<td>Identity and access management (IAM)</td>
<td>Current CSPs may not develop and implement adequate user access privilege controls.</td>
</tr>
<tr>
<td>Penetration detection</td>
<td>Consideration should be given to whether the CSP has a penetration detection system in use.</td>
</tr>
<tr>
<td>Compliance requirements</td>
<td>For the many compliance requirements—including privacy and PII laws, Payment Card Industry (PCI) requirements, or various financial reporting laws—today’s cloud computing services can challenge various compliance audit requirements currently in place. Data location, cloud computing security policy transparency and IAM are all challenging issues in compliance auditing efforts.</td>
</tr>
<tr>
<td>Public cloud server owners’ due diligence</td>
<td>Trust is a major component in the cloud computing business model. When contemplating transferring critical organizational data to the cloud computing platform, it is important to understand who and where all of the companies are that may touch the enterprise data.</td>
</tr>
</tbody>
</table>

Source: ISACA: IT Control Objectives for Cloud Computing - Controls and Assurance in the Cloud
References

• National Institute of Standards and Technology (NIST)
  http://www.nist.gov/index.html

• ISACA: IT Control Objectives for Cloud Computing - Controls and Assurance in the Cloud
  http://www.isaca.org

• Cloud Security Alliance
  http://www.cloudsecurityalliance.org
IT Audit Hot Topics: Integrated Auditing

June 25, 2013
What is Integrated Auditing?

An independent and objective audit that is performed by one integrated team, consisting of a combination of highly skilled staff from multiple disciplines to complete a thorough audit of business processes and issue a single audit report.
Benefits of integrating

- In-depth audit coverage
- Transfer, expand, and enhance knowledge sharing and cross training among auditors
- Management response addresses both process and technology issues
- Full transparency into details for the Audit Committee
- Limit customer fatigue
- Streamline and strengthening of the internal audit function, enabling it to deliver more strategic value
- Demonstration of a united audit division
Challenges with integration

- Cross functional management
- Getting business, IT and Forensic auditors focused on the same risk areas
- Talent gap in the industry for IT and analytic professionals
- Data access
- Aligning the timing of procedures
- Business and IT management involvement during the audit lifecycle
Key success factors

- Emphasize common business objectives
- Business, Technology and Forensic auditors should be held accountable for integrated audit targets in their performance goals
- Seamless integration amongst teams (communication, planning, schedules, etc.)
- The technology scope should be based on the key risks for the respective business processes
- Audit report should include feedback and approval from both groups
- Create a defined, repeatable integrated program
Future of Integrated auditing

- Integrated continuous auditing
- Business auditors with the knowledge necessary to perform entry-level IT application control testing
- Enhanced data analytics maturity
- Leveraging non-audit resources to gain expertise
Questions / Open Discussion

June 25, 2013