Top 10 Emerging IT Audit Issues: What keeps a CTO up at night
#1 Hack Attack
Hack Attack

Issues
• Rapid evolution of attack sophistication
• Broad footprint of attack vectors
• Targeted attacks via third-party vendors and spear-phishing are on the rise
• Budget constraints may prevent an adequate evaluation of the threat landscape and control implementation

Risks
• Regulatory violations resulting in fines
• Brand damage
• Loss of critical data or inability to restore operations

Recommendations
• Engage with executive management to address budget constraints
• Conduct a Cyber Assurance risk assessment and assign an audit relevance score to each audit area
• Prioritize audit areas based on the audit relevance score
# 2

Robotic Process Automation (RPA)
RPA in action

Issues
• Rapid evolution and adoption of RPA across the business to automate routine tasks
• Can serve a variety of purposes, more than just financial applications
• Potential for significant disruption
• Lack of standards or regulatory oversight

Risks
• Poorly designed solutions could result in regulatory violations, operational issues or financial losses
• Potential cyber exposure if malware is injected into the RPA code
• Routine IT platform changes may impact automation
• Lack of qualified support resources

Recommendations
• Discuss with management to understand existing RPA use
• Perform detailed risk analysis of planned RPA use
• Work with management to develop control solutions
• Consider using RPA in the audit function
#3

The new Collarless Workforce
The Collarless Workforce

**Issues**
- Enhanced/Artificial Intelligence and humans are beginning to work side by side
- Employee-only workforce model is becoming obsolete
- Many solution providers are making large investments in exploring business applicability
- Creates security, intellectual property (IP), platform consistency, and other issues

**Risks**
- Requires good data management and real-time data feeds
- Poor decision making, which may be automated
- Loss of critical business data
- Component integration challenges

**Recommendations**
- Understand current and planned use of cognitive technologies within the organization
- Determine what decisions will be driven off of cognitive platforms
- Assess risk commensurate with planned usage, including data management
Augmented Reality
Augmented Reality

Issues
• Augmented/Virtual reality technologies have arrived.
• Started primarily as consumer-based (e.g., smart glasses, smart phones).
• Moving into business-oriented applications.
• Potentially transformational.

Risks
• Full scope unknown
• Potential loss of data
• Failure to adapt
• Evolving control structure

Recommendations
• Discuss with application development team any potential movement toward virtual reality applications.
• Understand scope and functionality presented to determine risk profile and impact on controls.
• Define audit procedures.
• Consider impact on system development life cycle.
#5

Blockchain – Distributed Ledger
Distributed Ledger / Blockchain

Issues
• Data integrity issues via integrity-based attacks are an emerging risk
• Data confidentiality and safety
• Exchange assets safely and efficiently via self-governing digital “contracts”
• Cryptology may replace third party intermediaries as the keeper of trust

Risks
• Security standards and leading practices are not defined yet
• Legal recognition of contracts and digitally transferred assets is limited
• Security vulnerabilities within blockchain programming code or data path
• Evolving regulatory requirements and scrutiny
• Distributed architectures and open standards

Recommendations
• Work with management to determine what strategies and use cases they are pursuing or considering with blockchain
• Enhance or develop audit programs accordingly
Information in the Cloud(s)
Shadow IT
## Risk – In the cloud(s)

Organizations may not fully understand cloud risk

<table>
<thead>
<tr>
<th>WHO OWNS THE DATA?</th>
<th>IS IT SECURE?</th>
<th>WHERE IS IT STORED?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>66.9%</strong></td>
<td><strong>89.9%</strong></td>
<td><strong>40.7%</strong></td>
</tr>
<tr>
<td>Of cloud services do <strong>not</strong> specify that the customer owns the data in their terms of service*</td>
<td>Of cloud services do <strong>not</strong> support encryption of data at rest*</td>
<td>Of cloud services replicate data in <strong>geographically dispersed</strong> data centers*</td>
</tr>
</tbody>
</table>

Enterprises now have an **average** of 1,014 cloud services in use — and over 93% of those cloud services are not considered “enterprise-ready.”*

* Netskope, Inc. “June 2017 - Cloud Report”
Data in the Clouds(s)

**Issues**
- Rapid expansion of cloud adoption across the enterprise
- Cloud services are often inexpensive and may be acquired without additional approval
- New cloud services are created regularly
- Cloud storage may be located in undesirable geographic regions

**Risks**
- Data stored in the cloud may no longer be owned by the organization
- Legal and regulatory issues around data stored across international borders
- Potential increased cyber exposure

**Recommendations**
- Develop an understanding of current and planned deployment cloud services
- Audit the cloud vendor selection process and understand the minimum controls baseline
- Evaluate risks based on type of data and planned usage
- Design corresponding consultative and assurance procedures.
Data is currency
Data is currency

**Issues**
- Increased scrutiny of data life cycle management by regulators, auditors, customers, employees, and business partners
- Issue is exacerbated due to device proliferation, cloud support, emerging malware technologies, evolving regulatory requirements, and file-sharing solutions

**Risks**
- Fines, financial impacts
- Brand damage
- Loss of critical data
- Preparedness for compliance with California Consumer Privacy Act (CCPA) 1/1/2020

**Recommendations**
- Conduct additional Data Governance audits (e.g. Data Classification, Records Record Retention)
- Move to a programmatic approach to auditing, similar to cyber risk.
- Begin with organization policies and taxonomies.
- Review linkages to relevant laws and regulations.
- Evaluate storage and defensible destruction requirements.
- Evaluate linkage to bring-your-own-device management policies and procedures.
#8

Internal Audit Agility
Agile, Analytics and Approach to Auditing Agile Processes

**Issues**
- IA may not be seen as adding value in areas of higher importance to the business
- IA focus can be rigid with too much time spent in non-value areas
- It’s not always a collaborative process and responsive to emerging risks/needs
- The audit approach may need to shift when a processes change

**Risks**
- Effective management of an increased risk landscape with limited funding
- It’s a new concept – change management should not be underestimated
- IA leadership may not fully support a transformational commitment
- Team members not comfortable with less structure and more empowerment
- When a process changes controls may no longer mitigate the risk effectively

**Recommendations**
- Train your IA team on Agile methodology and apply to IA approach
- Develop resources as scrum masters
- Select some pilot projects on your IA plan to test out the approach
- Pick pilot projects wisely – having a collaborative business partner is key
- Review controls when a process changes (Ex: Development group moves to Agile and Dev Ops)
#9

Board / Audit Committee Confusion
Board / Audit Committee Confusion

Issues
• Board awareness of Information Security / Cybersecurity risks are increasing
• These programs require an assurance component, lacking in many organizations
• Evolving standards and regulations will make this even more critical for IA (e.g., Securities & Exchange Commission cyber disclosure, AICPA cyber examination, SOX cyber amendment)
• Customers and shareholders expect that the appropriate things are being done

Risks
• Board members aren’t able to make the right decisions
• False reliance on inaccurate security metrics
• Impact to brand and reputation if breaches or incidents occur
• Loss of critical or confidential data puts everyone at risk

Recommendations
• Work with the board and/or audit committee members on how they want to see metrics
• Measure the effectiveness of both technology and security programs
• Report to the board and/or audit committee using easily digestible and transparent reporting methods
IT/Cyber Assurance reporting example

- Allows stakeholders to communicate effectively
- Provides “at a glance” status update
- Customized for each group of stakeholders
#10

Sensor Proliferation
Sensor proliferation

Issues
• Rapid expansion of distributed sensor nodes, which in turn can help drive and/or control events
• May or may not be connected to the Internet of Things (IoT)

Risks
• Effective management of very large numbers of sensors in and out of the enterprise
• Effective data usage processes and policies
• Variety of risks related to inoperable sensors
• Potential increased cyber exposure

Recommendations
• Develop an understanding of current and planned deployment of sensor technologies within your environment.
• Understand your organizations sensor strategy and how you will ingest sensor data
• It’s coming, plan for it!
• Evaluate risks based on type of sensor and planned usage and design corresponding consultative and assurance procedures.
Questions