TECHNOLOGY AND AUDIT: A MUTUAL FUTURE

THERESA GRAFENSTINE
CHAIR, ISACA BOARD OF DIRECTORS
AGENDA

THE AUDIT LANDSCAPE

PROCESSES AND TRENDS

CHANGES

LOOKING FORWARD

AUDIT OF THE FUTURE

ENTERPRISE OF TOMORROW

FOCUS ON THE FUTURE

FOCUS ON RESILIENCE
EVOLUTION OF IT AUDIT

Regulatory has been a major driver:

- SOX
  - Financial reporting
- HIPAA
  - OCR/RAC audits
- PCI DSS
  - Cardholder data requirements
  - Annual report on compliance (or self-assessment)

“It is important to understand that future leaders in the IT Audit profession must be open to developing skills beyond traditional IT risk and control knowledge as technology continues to synergize with emerging business expectation”

WALT BLACKWOOD
CISA, COL(R)
Senior Director, IT Audit,
Internal Audit, TIAA,
Financial Services
THE PROFESSION IS CHANGING

Challenges:

- Pace of changes
- Audit scope expansion
- New business models and ways of doing things
- Increasing technical sophistication
- Resourcing

“Audit committees should be aware of cybersecurity trends, regulatory developments and major threats to the company, as the risks associated with intrusions can be severe and pose systemic economic and business consequences that can significantly affect shareholders.”

ROSEMARY M. AMATO
CISA, CMA
Audit Committee Chair for the Institute of Management Accountants (IMA) and Director Deloitte Netherlands
Survey key findings:

- Cybersecurity is the top challenge
- Increasing executive interest in IT audit
- CAE’s carrying leadership for IT audit directly
- Most IT auditors involved in key technology projects
- Most perform audit risk assessment; majority do so annually
PROCESSSES AND TRENDS IN IT AUDIT

Enterprise risk management (ERM)

Supply chain risk management
Assurance of partners
Supply chain relationships

Corporate governance
Extends to IT governance

Source: 2017 ISACA/Protiviti Study: A Global Look at IT Audit Best Practices
ADDITIONAL TRENDS IN AUDIT TO LOOK FOR, SHORT-TERM
ROBOTIC PROCESS AUTOMATION (RPA) AND COGNITIVE INTELLIGENCE (CI)

Increasingly being adopted in business and ‘second-line’ functions, particularly in data-driven or data-intensive industries, such as financial services

Audit can support RPA and CI implementations by being proactive in identifying, assessing and monitoring risk(s) of these technologies; requires understanding of a new risk landscape

RPA can be used to automate repetitive controls testing and internal reporting tasks, but first, auditors should ascertain the effect(s) of RPA and CI on existing processes, on management, and on the enterprise as an entity—and this means involvement early in the adoption of these technologies, not later

Source: various authors: Internal Audit Insights 2018: High-Impact Areas of Focus; Deloitte, January 2018
ADDITIONAL TRENDS IN AUDIT TO LOOK FOR, SHORT-TERM

**ANALYTICS**

Has always been a significant force in audit, but lately has evolved into one of the most important strengtheners of audit efficiency and effectiveness; this only becomes more important with the increasing digitization of business.

With that increasing digitization also comes increased stakeholder need for stronger risk anticipation, better insights, and greater assurance.

Analytics and visualization tools for data are becoming less expensive, more user friendly, and more prevalent in the marketplace.

Focus of audit can and should be on **generating relevant insight**, not merely a list of exceptions; use of RPA and CI has a role to play in analytics efforts, automating tasks and accelerating reporting (as well as improving it).

**Source:** various authors: *Internal Audit Insights 2018: High-Impact Areas of Focus; Deloitte, January 2018*
Cybersecurity audits have traditionally examined regulatory compliance; the most significant risks now, though, are coming from the cloud, from external contractors, and from shadow IT.

Challenge lies in identifying cyber risk before it occurs; critical to fold in organizational culture as well, to ensure employee decisions and behaviors minimize cyber risk.

Consider ‘war gaming’ or operational exercises to test how cyber incidents will impact data, infrastructure, operations, and financial/reputational assets; gauge responses and resilience.

Source: various authors: Internal Audit Insights 2018: High-Impact Areas of Focus; Deloitte, January 2018
CYBER SECURITY MATURITY ASSESSMENT

BENEFITS AND IMPACT

**STANDARDIZED MATURITY**
- Defines maturity for people, process and technology; includes hygiene; enables industry benchmarking

**COMPANY RISK-BASED**
- Defines company’s risk profile and sets maturity targets

**ROADMAP DEVELOPMENT**
- Provides risk-based prioritization of gaps in maturity to support roadmap development

**COMPLIANCE VIEWS**
- Provides views into compliance with ISO27001, NIST CSF, CMMI Threat Kill Chain, ASD, etc.

WE PRESENT OUR RESULTS IN
BUSINESS TERMS
SIMPLE GRAPHICS TO SUPPORT BOARD COMMUNICATION

OUR COMPREHENSIVE SCOPE
LEVERAGES LEADING FRAMEWORKS, STANDARDS AND CONTROLS
INCREASING TECHNICAL SOPHISTICATION

Technical sophistication required by audit teams necessary to assess new technologies

Artificial Intelligence (AI)
Robotics

New methods required for conducting audit

Data visualization
Machine learning

Source: 2017 ISACA/Protiviti Study: A Global Look at IT Audit Best Practices
The Rise of Shadow IT

Shadow IT and “Consumerization” of technology impacts the role of CIO

No longer about finding and deploying solutions

A strategic partnership that incorporates new technology coming in and aligns it with solutions already in place

Shadow IT Adoption Lifecycle

**Solo** phase
- Individual use
- Used in isolation
- Limited use scenarios

Small team phase
- Usage broadens
- Small teams
- Usage integrates into broader workflow

Integration
- Small teams join forces as usage grows
- Usage integrates between teams and other apps

Standardization
- Usage becomes enterprise-wide
- Part of normative operations
PACE OF CHANGES

Rapid technology and footprint expansion
Cloud
Mobile
IoT

Increasing agility/velocity
DevOps

…but audit planning has stayed stagnant(ish)
1 year audit planning cycle
6 month (or longer) risk review

Source: 2017 ISACA/Protiviti Study: A Global Look at IT Audit Best Practices
ON THE HORIZON?

Networked industries
Networked everythng
Networked society

Networked consumer electronics

Image source: Erikson
THE AUDIT OF THE FUTURE

What’s required?

People
Require different, more finely-honed skills

Process
Better audit planning

Technology
Advanced toolset, hands-on approaches
HOW RISK GETS EVALUATED

To evaluate an auto’s safety, you need to learn/understand:

- Automobile operation (steering, braking, etc.)
- Rules of the road
- Traffic laws
- Road conditions/weather
- Safety features (seatbelts/airbags)
- Tire conditions/pressure
- Engineering of braking/steering systems
- Service/maintenance history
- Traffic laws
- Etc. (too many other things to list)

The implication: Assessing risk takes longer and requires more data compared to understanding usage. Requires evaluation of people/process/technology.
PEOPLE (SKILL DEVELOPMENT)

Increased technical understanding
Required given complexity expansion in environments

Better business understanding
Understand what the business does and how it does it

Integration and crossover with:
Security (physical and logical)
Compliance (legal, HR, privacy)
Risk (risk operations, risk planning, ERM)
Faster audit planning

*Will a 1 year planning cycle be enough, going forward?*

Consider: Some companies in the digital economy are making production code changes every minute of every day, throughout the year.

*Will an audit plan hold up, some 525,600 code changes later?*

Moves to continuous audit

Increased automation

Integration with automation happening in other areas (e.g. DevOps)
New, better ways of:
- Analyzing evidence
- Collecting artifacts
- Understanding risks

Examples:
- Data visualization
- Determining “safe” AI
- Automating assessment to minimize resource consumption
THE ENTERPRISE OF TOMORROW

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
DIGITAL ENTERPRISE
AUDITS IN DIGITAL ENTERPRISE

Audit of the future
Concurrent to business process
Multi temporal PoV
Limited lag between reporting and action on findings
Need for real-time or near-real-time actions

Audit

Business process

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
Evolving Aspects of Audits

- Auditor
  - Competency
  - Independence

- Auditee
  - Non-human auditees

- Scope of the Audit
  - Traditional scoping may no longer apply
  - Scoping
    - Evidence collection & retention
    - Usage of tools

- Audit process

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
Audit implications from the digital enterprise

Audit is concurrent/"real-time"

Evidence management
Approaches to obtaining evidence will change
Evidence analysis, retention will change

Corrective action time frames change radically
Actions required “real-time” or “near-real-time”

Blurring of audits/reviews/monitoring

Increased integration between business and ‘audit’

Need for increased audit skepticism

Need for high quality audits /increased reliability

Contextual reporting v/s binary reporting

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
AUDIT OF THE DIGITAL ENTERPRISE: FUTURE FOCUS

Business process risk management

‘Strength’ of controls

Change management

Configuration control

Increasing need to use analytics

Coalesced insights drawn from multiple sources

Ability to analyze larger sets of data rather than sampling

Audit ‘intelligence’

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
IMPLICATIONS FOR THE AUDIT PROFESSIONAL

Outsider to trusted, valued insider

Collaborate more / Share knowledge

Keeps abreast of changing technology

Possess high domain knowledge.

Uses tools extensively.

Be closely attached to the business process... without impinging on independence

Engage before and during the course of business rather than only post facto.

Increasing need to involve in post audit actions

Source: Auditing the Digital Enterprise: (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
IMPLICATIONS FOR THE AUDIT PROCESS

Increasing reliance on rules/parameterization

Embedding of audit routines into the business process

On-going collection of evidence & analysis

Emphasis on evidence collection/analysis /retention

End-to-end audit life cycle management tools

Go with the flow of business process rather than against the grain

Deep, wide and technical- all need to be ticked

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
MODELED OUTCOMES

Audit strategy aligned with business strategy
Move from a line of defense to a strategic value adding role
Improved audit productivity
Increased automation

Consistency across teams, businesses, geographies
Enhanced audit management ability
Analytics leveraged to identify trends
Predict areas of higher risk
Become force multipliers
Metrics to drive, deliver and demonstrate value

Source: Auditing the Digital Enterprise; (Presentation of RV Raghu at 2017 ISACA Asia Pacific CACS)
THANK YOU...

QUESTIONS?