IS AUDIT & CONTROL MAIN CONCEPT

CINDY HIMAWAN

1

WHY?

Increased Organizational Complexity

- strategic workforce planning
- Organizational resilience
- risk culture

Heightened Stakes for Managing and Protecting Data

- data governance
- data privacy

Digital Business Transformation

- cyber vulnerabilities
- artificial intelligence
- IT governance
- standardized and effective project management

Heightened Geopolitical and Regulatory Volatility

- regulatory developments
- supply chain network
- third parties organizations work with

What is IS Audit Control?

IS

The system used in the organization to proceed information become valuable output

AUDIT

systematic process of **objectively obtaining** and evaluating **evidence** regarding **assertions** to **ascertain the degree of correspondence** between those assertions and established **criteria** and **communicating the results** to interested users

CONTROL

control system comprises **policies**, **practices**, and **procedures** employed by the organization to achieve **objectives**

IS Audit Control is evaluation of technology, practices, and operations in the system used to assure the integrity, validity and reliability of an entity's information and to ensure the continuity of the evaluated process

Audit Plan Hot Spots Summary

Audit Plan Risk Areas	Summary	2020 Drivers
IT Governance	Organizations are undertaking technology initiatives critical to their growth or even their survival. As organizations continue to look to IT to advance business strategy and initiatives, IT governance is even more important. Poor IT governance can lead to project failure, security vulnerabilities in mismanaged IT assets and operational delays.	1. RPA Governance Challenges 2. Piecemeal Modernization of Legacy Systems
Regulatory Developments	Regulatory risk continues to be a top concern for companies. Divergent regulations spanning various geographies and levels of government present a challenge as companies grapple with new compliance requirements. At the same time, companies report compliance activities have become more onerous in the past few years and expect this trend to continue. **This is an evolution of last year's regulatory uncertainty hot spot.**	1. Regulatory Focus on Cybersecurity 2. Waste Reduction and Climate Resiliency
Organizational Resilience	Organizations that nimbly adapt and respond to business incidents can lower their impact and decrease recovery time. However, siloed risk management and poor cross-functional collaboration hamper effective responses to business interruptions. Additionally, insufficient focus from board leadership may result in inadequately funded business continuity functions and contribute to disjointed responses in a crisis. **This is an evolution of last year's operational resilience hot spot.**	1. Fragmented Risk Management 2. Lack of Board Attention to Resiliency Practices
Supply Chain	Many organizations have combined globally distributed supply chains with lean processes heavily dependent on a small number of suppliers. The fragility of these supply chains means supplier risk events can hinder organizations' access to vital materials, and increases in extreme weather and trade restrictions make such supplier risk events more likely.	1. Environmental Disasters 2. Tariffs and Trade Policy
Strategic Workforce Planning	Organizations' pursuit of digital initiatives, combined with changing employee expectations, are requiring employers to reevaluate workforce strategies. To remain competitive in a tight labor market and evolving business environment, organizations are increasingly adopting remote work arrangements, employing more contingent workers and trying to reskill employees to meet changing skill demands.	1. Workforce Reskilling Challenges 2. Growth in Nontraditional Working Arrangements
Artificial Intelligence (AI)	Investments in AI are on the rise as organizational leaders are keen to tap into the ability of AI to fundamentally change how they do business. While some benefits, such as workflow improvements and enhanced data insights, are being achieved, AI algorithms can lead to a range of regulatory, ethical and security challenges.	1. Unintended Consequences of AI 2. Vulnerabilities of AI Algorithms

Audit Plan Hot Spots Summary

Audit Plan Risk Areas	Summary	2020 Drivers
Data Governance	Even as the strategic importance of data grows, few organizations have a formal data governance framework in place, which could enable more effective management and use of data. The absence of data governance is leading organizations to misallocate resources, produce poor quality insights and miss potential business opportunities.	1. Data Overretention 2. Insufficient Preparation for Data Migration
Third-Party Ecosystems	The number and diversity of third parties that organizations are working with continues to rise. However, as organizations entrust these parties with more critical tasks and greater access to organizational data, monitoring practices haven't kept pace. Failures at third parties are more costly than ever for organizations, as regulators and consumers are raising the stakes in terms of organizational accountability. **This is an evolution of last year's third parties hot spot.**	1. Extension of Liability 2. Deeper Entanglement of Third Parties
Cyber Vulnerabilities	Cybercriminals now operating like syndicates with a variety of low-cost hacking tools at their disposal has resulted in a growing number and scale of cyberattacks. Organizations are largely unprepared to detect and respond to most of these attacks as challenges with skills, budget and foundational security measures persist. **This is an evolution of last year's cybersecurity preparedness hot spot.**	1. Employee Security Behaviors 2. Cyber-Physical Convergence
Data Privacy	As organizations collect more data to make strategic decisions, data privacy risk expands. This is underscored by recent high-profile data breach incidents and record-breaking fines. Regulators are reacting with a growing patchwork of data privacy regulations throughout the world with more on the horizon, significantly increasing complexity and the cost of compliance.	1. Increasing Regulatory Complexity 2. Underestimation of the Need to Protect Employee Data
Risk Culture and Decision Making	Risk culture and its effects on corporate decision making are gaining increased attention from regulators and societal institutions at large. The ability for the business to make risk-informed decisions will only become further challenged as risks grow more connected and the next recession looms.	1. Complexity and Interconnectedness of Risks 2. Looming Economic Downturn
Project Management	Despite decades of relying on high-impact projects, few organizations report high project management maturity. As organizations increasingly rely on projects to help them remain relevant and competitive, better enterprisewide and strategic coordination is imperative to reduce waste and help support business objectives.	1. Ill-Defined Project Strategies 2. Siloed Project Execution

AUDIT TRENDS CHANGES

	Current state	Future state
Value drivers	Audit plan coverage	Dynamic risk coverage
Audit's role	Providing the board with assurance	Business risk partnership
Business role	Bolt-on risk management	Built-in risk management
Delivery model	On-site, point-in-time auditing	Digital auditing
Resources	Audit-expertise-driven structure	Operational-expertise-driven structure

Top audit department priorities

Percentage of respondents rating priority as important to extremely important

Priority	Percentage
Detect and assess emerging risks	87%
Stakeholder relationships	83%
Data analytics	83%
Audit productivity	77%
Audit talent management	72%
IT auditing	72%
Optimization of audit department	63%
Continuous auditing and monitoring	60%
Balancing regulatory demands with risk-based auditing	50%

0%   50%   100%

AUDITOR CLASSIFICATIONS

Internal audits and assessments

- This involves auditing your own organization to discover evidence of what is occurring inside the organization (self-assessment)
- **Audit** an audit generates a report considered to represent a high assurance of truth
- **Assessment** an assessment is less formal and frequently more cooperative with the people/objects under scrutiny. Its purpose is to see what exists and to assess value based on its relevance.

External audits

- The business audits its customer or supplier, or vice versa
- The goal is to ensure the expected level of performance as mutually agreed upon in their contracts
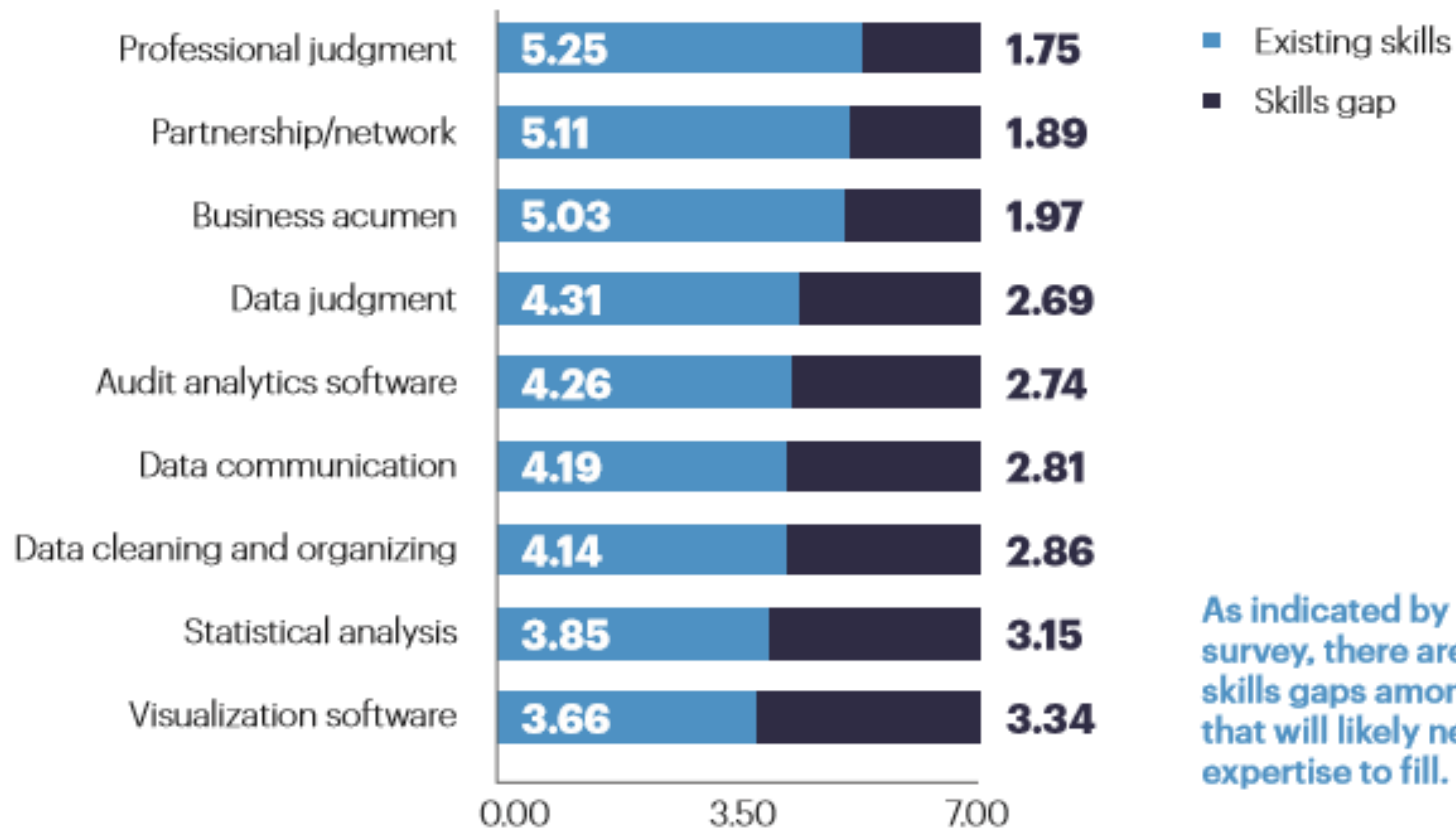
Independent audits

- Outside of the customer-supplier influence
- frequently relied on for licensing, certification, or product approval

EXTERNAL VS INTERNAL AUDITOR

- **External auditors** often called independent auditing because it is done by certified public accountants who are independent of the organization being audited.

- External auditors represent the interests of third-party stakeholders in the organization, such as stockholders, creditors, and government agencies.

- Usually the focus of external audit is on financial statements, this type of audit is called financial audit

- **Internal auditors** can add enormous value to an organization by providing ongoing efforts that help prepare the organization for an external audit.

- The internal auditor could approach the situation with an attitude of independence even though they will be unable to certify or attest final results.

- Their expert audit skills could help guide design and remediation efforts at a substantially lower cost than that of their external counterparts.

Skills of auditors

Effectiveness rating of 1 – 7

Skill	Existing skills	Skills gap
Professional judgment	5.25	1.75
Partnership/network	5.11	1.89
Business acumen	5.03	1.97
Data judgment	4.31	2.69
Audit analytics software	4.26	2.74
Data communication	4.19	2.81
Data cleaning and organizing	4.14	2.86
Statistical analysis	3.85	3.15
Visualization software	3.66	3.34

■ Existing skills
■ Skills gap

0.00   3.50   7.00

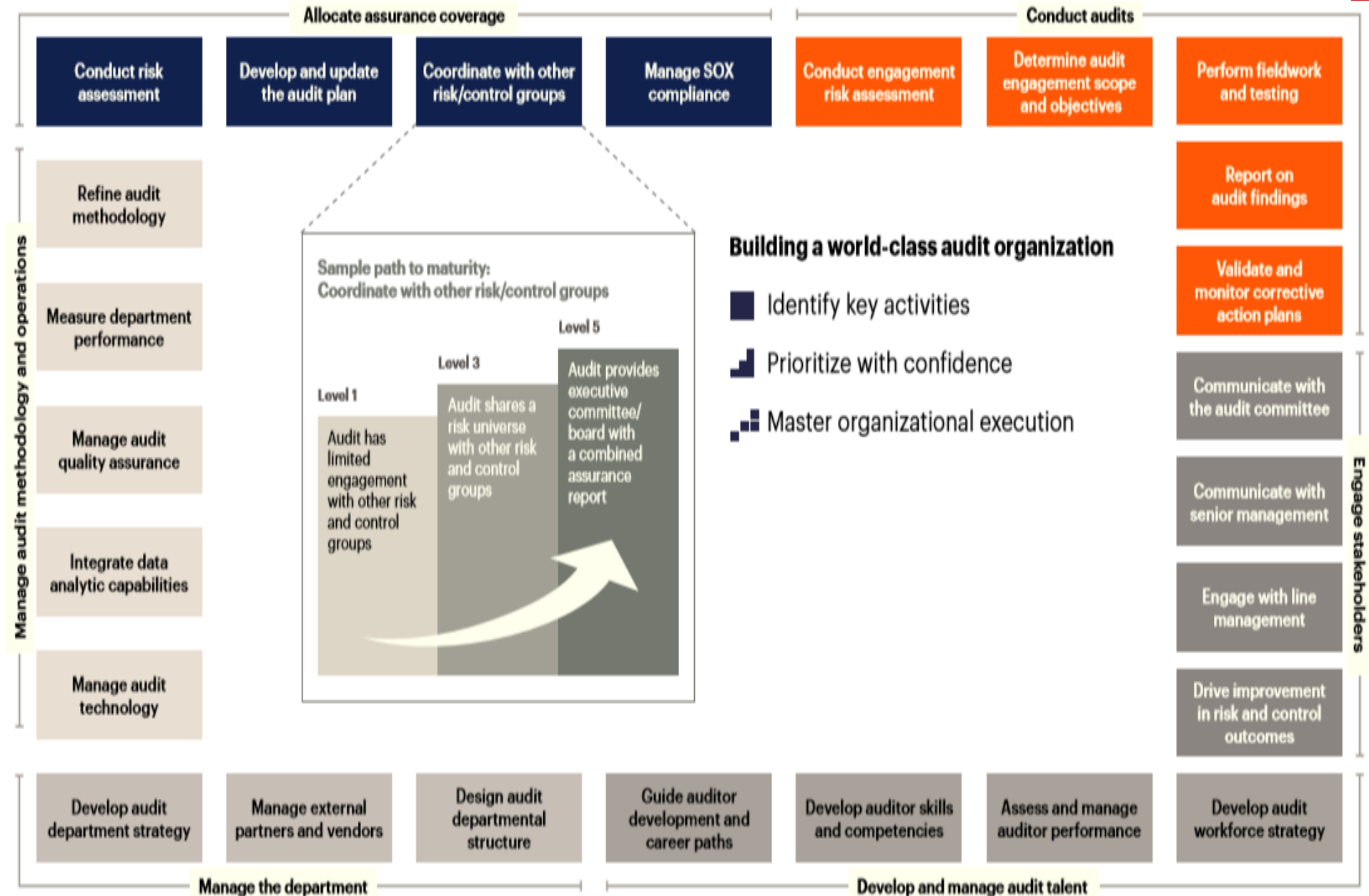**As indicated by our recent survey, there are significant skills gaps among auditors that will likely need external expertise to fill.**

n = 232
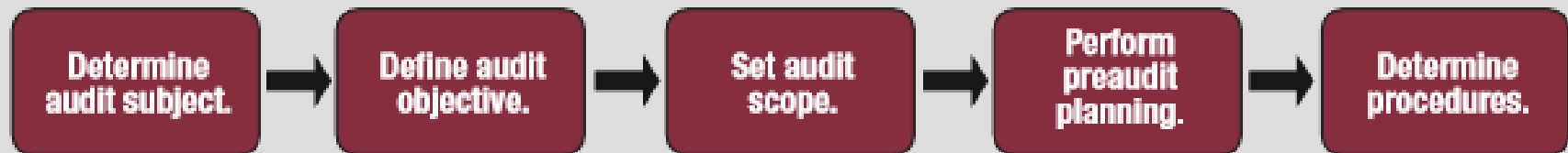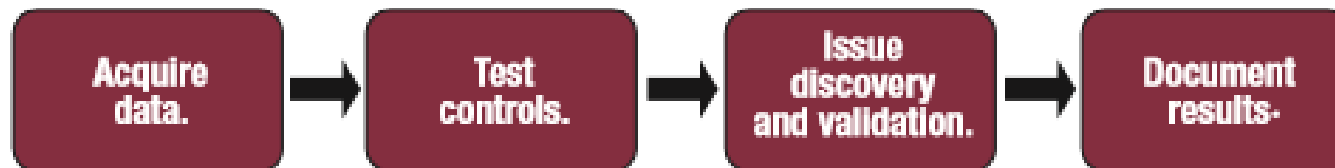Source: Gartner Audit 2017 Data Analytics in Audit Benchmark

11

AUDIT ACTIVITY

Allocate assurance coverage

Conduct risk assessment	Develop and update the audit plan	Coordinate with other risk/control groups	Manage SOX compliance

Conduct audits

Conduct engagement risk assessment	Determine audit engagement scope and objectives	Perform fieldwork and testing

Manage audit methodology and operations

- Refine audit methodology
- Measure department performance
- Manage audit quality assurance
- Integrate data analytic capabilities
- Manage audit technology

- Report on audit findings
- Validate and monitor corrective action plans

Engage stakeholders

- Communicate with the audit committee
- Communicate with senior management
- Engage with line management
- Drive improvement in risk and control outcomes

Sample path to maturity: Coordinate with other risk/control groups

Level 1
Audit has limited engagement with other risk and control groups

Level 3
Audit shares a risk universe with other risk and control groups

Level 5
Audit provides executive committee/ board with a combined assurance report

Building a world-class audit organization

- Identify key activities
- Prioritize with confidence
- Master organizational execution

Manage the department

Develop audit department strategy	Manage external partners and vendors	Design audit departmental structure

Develop and manage audit talent

Guide auditor development and career paths	Develop auditor skills and competencies	Assess and manage auditor performance	Develop audit workforce strategy

AUDIT PROCESS - ISACA

Figure 2—Typical Audit Process Steps by Phase

Planning Phase

Determine audit subject. → Define audit objective. → Set audit scope. → Perform preaudit planning. → Determine procedures.

Fieldwork and Documentation Phase

Acquire data. → Test controls. → Issue discovery and validation. → Document results.

Reporting Phase

Gather report requirements. → Draft report. → Issue report. → Follow-up.

STRATEGIZE YOUR AUDIT PLAN

1 Statement of strategy.
Craft a clear, concise and memorable statement that captures the essence of the functional strategy and summarizes the key objectives on which your function will focus in the coming one to three years to enable business strategy.

2 State of the function.
Identify the best indicators (four to seven key performance measures) to describe the performance of the function today and its desired future state.
• Capabilities. include a list of (three to five) capabilities their function needs in order to support enterprise ambitions.

3 Top urgency drivers.
Specify one or two key trends driving the change in business conditions to which the business and your function must respond.

4 Top functional initiatives.
List the top four to seven key initiatives required for your function to achieve its desired end state.

5 Critical assumptions.
Document critical assumptions underpinning your strategy. Limit the number and be prepared to set metrics and thresholds where necessary to indicate when course correction is required as circumstances change.

① Statement of Audit Strategy

Create value for the business by leveraging internal control expertise to drive process improvement and improve risk management. As a valued strategic partner, we strive to help the business achieve its operational, reporting and compliance objectives.

② State of Audit in 20XX

Top Four to Seven Metrics Describing Initial State

- Percentage of key risks covered by internal audit in the audit plan: 60%
- Client satisfaction: 70%
- Issues self-disclosed by management: X
- Process improvements implemented by business: X
- Audit staff with data acumen: 25%
- Time saved through use of technology: 3,000 hours
- Complete assurance map with other assurance providers

③ Top Urgency Drivers (one or two)

1. Organizational change fueled by digitalization and automation is making it harder to provide on-time assurance.
2. Audit capabilities and skill gaps do not meet shifting assurance needs.

④ Audit Initiatives (four to seven)

1. Improve audit productivity and output to accommodate the speed and interconnectedness of the business.
2. Recruit, attract and develop new skill sets to meet changing risk coverage needs.
3. Expand coverage of key risks by better coordinating with "second-line" assurance groups and enabling greater business risk ownership.
4. Mature and grow data analytics capabilities.

⑤ Critical Underlying Beliefs and Assumptions

1. Budgets for internal audit departments are likely to remain flat.
2. Accelerating company growth will put new and unpredictable risks into play that stakeholders haven't anticipated.
3. Use of data analytics will improve audit outcomes, productivity and risk assessment capabilities.
4. Audit teams will need to rely on the second line and first line to better monitor risks and controls.
5. Internal audit needs to link its audit outcomes to value contribution and process improvements to demonstrate its impact on the business.

② State of Audit in 20XX

Top Four to Seven Metrics Describing End State

- Percentage of key risks covered by internal audit in the audit plan: 80%
- Client satisfaction: 85%
- Issues self-disclosed by management: 2X
- Process improvements implemented by business: 2X
- Audit staff with data acumen: 55%
- Time saved through use of technology: 10,000 hours
- Rely on other assurance providers for X% of coverage