Rethinking risk assessment and the IA plan

November 2020
Administrative

- Require that online participants take part in online questions.
- Must respond to a minimum of three questions per 50 minutes.
- Polling questions will be pushed via Zoom.
- Results will be reviewed in the aggregate; no responses will be tracked back to any individual or organization.

Ask a question
- Use the “Chat” box in your Zoom window.

Technical issues
- If technical support is needed, please submit a question through the Chat box.
With you today

Stephanie Isaacson
Managing Director, Internal Audit & Enterprise Risk

Sheila Stark
Director, Internal Audit & Enterprise Risk, Internal Audit Reimagined Leader

Chris Launey
Manager, Internal Audit & Enterprise Risk, Data Hub and Internal Audit Reimagined teams

KPMG hosts
Learning objectives and agenda

**Learning objectives**

- Articulate the benefits of innovating within the risk assessment process for improved planning
- Identify where innovation can be incorporated into the risk assessment process, in incremental steps based on current state

**Agenda**

- Case for change
- Introduction to guiding principles for innovation
- Incremental steps
- Show and tell
What is your case for evolving?

Audit committee perspectives®

— Robust risk management program in place, may not capture disruptive risks
— Maintain flexibility in internal audit plan to adjust to changing business and risk conditions
— Focus internal audit plan on other key areas of risk and related controls

Internal audit perspectives®

— IA plan is adaptive to changes in the landscape with varying mix of risks efforts.
— Continuous risk monitoring capabilities in place alongside point-in-time risk assessment efforts
— Deeper insights incorporated through data analytics and technology.

Be a strategic adviser
Identify the right risks – Perform the right audits – Achieve the mission of internal audit

① Top responses from the KPMG 2019 Audit Committee Pulse Survey of more than 200 audit committee members: https://boardleadership.kpmg/us/relevant-topics/articles/infographics/keeping-pace-with-disruptive-risk-digital-transformation.html
② Top audience responses from KPMG web event, November 2020; total approximately 1000 IA professionals as participants
Benefits of change

Be a strategic adviser
Identify the right risks – Perform the right audits – Achieve the mission of internal audit

Assess risk at a frequency closer to the pace it changes
Leverage data and technology like other functions in the organization
Maintain a plan with audit topics and approaches aligned to risk status and strategic direction of the organization

Demonstrate and visualize audit efforts to protect and enhance business value
Provide independent, organization-wide view of risk for agility in approach

Assess risk at a frequency closer to the pace it changes
Unlocking innovation across the approach

The IIA standard risk assessment and IA planning process

Our vision: Risk assessment and IA planning that is proactive, data driven, and dynamic

Guiding principles to achieve this vision:

1. Mindset and **strategy** shift from defensive to proactive
2. **Deeper insights** are incorporated through use of data analytics and technology.
3. **Risk** is more frequently assessed.
4. Continuous **risk monitoring** and sensing capabilities are in place.
5. **IA plan** is adaptive to changes in the risk landscape.
6. **Alignment** with other risk functions

© 2020 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP127066-1A
CPE questions

Where do your stakeholders most indicate an interest in your current approach evolving?

A. Current approach is good as is

B. Interest in more proactive identification of risk, including emerging and disruptive risks

C. Interest in better leveraging data analytics for risk insights

D. Interest in more frequent risk assessment and/or agility to the internal audit plan

D. Interest in increased risk insights overall, to drive more informed decision making
### Achieving the guiding principles

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Defensive, limited risk domains</td>
<td>Limited qualitative and manual</td>
<td>No formal risk assessment</td>
<td>None</td>
<td>No formally approved plan</td>
</tr>
<tr>
<td>Defensive, expanded risk domains</td>
<td>Expanded qualitative and manual</td>
<td>Performed annually; simplistic measurement</td>
<td>Very limited data and domains (internal)</td>
<td>Static plan for limited risk domains</td>
</tr>
<tr>
<td>Defensive, some proactive</td>
<td>Qualitative and limited quantitative; partial tech. enabled</td>
<td>Performed ≥ annually; formal measurement</td>
<td>Expanded data and domains (internal)</td>
<td>Static plan across risk domains, reconsidered as needed</td>
</tr>
<tr>
<td>Defensive and proactive</td>
<td>Quantitative and expanded qualitative; tech. enabled</td>
<td>Performed &gt; annually; enhanced measurement</td>
<td>Expanded data and domains (internal and external)</td>
<td>Partially dynamic plan with periodic updates</td>
</tr>
<tr>
<td>Proactive across risk domains</td>
<td>Balanced quantitative and qualitative; tech. enabled</td>
<td>Continuous assessment with enhanced measurement</td>
<td>Continuous monitoring processes across domains</td>
<td>Fully dynamic plan, updated regularly</td>
</tr>
</tbody>
</table>

### 6. Alignment with other risk functions as an inhibitor or accelerator

- Ad hoc
  - Developing
  - Capable
  - Savvy
  - Optimized

© 2020 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP127096-1A
Questions thus far?
Incremental steps
Where to start the incremental steps

Typical flow of risk assessment and IA plan

1. Define risk and audit universe
2. Collect risk insights
3. Perform risk analysis
4. Identify audit topics
5. Draft plan and resources
6. Approve and execute plan
7. Reassess plan as needed

Incremental steps for innovation, start with one or multiple

- Shift or expand risk focus
- Expand sources of insights
- Introduce technology and monitoring
- Change nature of audit efforts
- Shorten duration of plan
- Utilize alternative resourcing
- Increase frequency of reassessing
Incremental steps

Risk universe and risk insights

Some steps to consider:
— Shift or expand risk focus to address areas most likely to impact business success, such as Strategic
— Expand sources of insights used beyond interviews and limited quantitative indicators

Key qualitative indicators | Early quantitative indicators
---|---
Corporate strategy | Capital investments

Key qualitative indicators | Early quantitative indicators
---|---
Head count and turnover | Tenure of management positions

Key qualitative indicators | Early quantitative indicators
---|---
Technology strategy and initiatives | IT incidents and change history
IT threat intelligence data | Technology asset register

<table>
<thead>
<tr>
<th>Key qualitative indicators</th>
<th>Early quantitative indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal control design or operating effectiveness issues and deficiencies</td>
<td>General ledger balances</td>
</tr>
</tbody>
</table>
Quarterly certifications | |

---

© 2020 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP127066-1A
**Risk analysis**

**Incremental steps**

1. Define risk and audit universe
2. Collect risk insights
3. Perform risk analysis
4. Identify audit topics
5. Draft plan and resources
6. Approve and execute plan
7. Reassess plan as needed

---

**Some steps to consider:**

- Introduce technology and monitoring

---

**Mapping Risk across COMPANY Auditable Entities**

Following table shows an example mapping of risk focus areas to the COMPANY auditable entities.

---

**Internal Audit Risk Ranking Analysis**

- **Severity** ([Highest Rating to Lowest Rating])
  - Reimbursement Levels
  - Physician Comp.
  - Revenue Cycle Management

- **Likelihood** ([Highest Rating to Lowest Rating])
  - Reimbursement Levels
  - Physician Comp.
  - Revenue Cycle Management

- **Velocity** ([Lowest Rating to Highest Rating])
  - Physician Comp.
  - Revenue Cycle Management

- **Mitigation Effectiveness** ([Lowest Rating to Highest Rating])
  - Physician Comp.
  - Revenue Cycle Management

---

**Legend:**

- **1.** Introduction and Design
- **2.** Business Continuity & Incident Management
- **3.** Change Management
- **4.** Data Governance
- **5.** Enterprise Architecture
- **6.** Enterprise Risk

---

**Additional Resources:**

- [KPMG LLP](https://www.kpmg.com)
- [KPMG Global](https://www.kpmg.com/global/en)
- [KPMG International Limited](https://www.kpmg.com/international/en)

---

© 2020 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP127066-1A
Risk analysis (continued)

Some steps to consider:
- Introduce technology and monitoring

Data tools
- Alteryx
- Excel
- SQL

Risk insights
- Identify and gather metric data
- Metric data transformation
- Capture qualitative risk insights
- Validate/refine risk scoring

Visualization tools
- Power BI
- Qlik
- Tableau

Risk analysis and audit topics
- Review and interpret results
- Apply historical audit knowledge
- Identify audit topics

Draft and manage audit plan
- Draft dynamic audit plan
- Resource planning
- Approve and execute plan
- Monitor progress of plan and map results to risks

Platform tools
- AuditBoard
- Oracle
- SAP
- ServiceNow
- TeamMate
- Workiva
Incremental steps

Identify audit topics and draft plan

Some steps to consider:
- Change nature of audit efforts
- Shorten duration of plan

[Diagram showing top audit plan topics by risk ranking with heat map key]

Proposed audit projects
1. Audit topic 1 (collaborate)
2. Audit topic 2
3. Audit topic 3 (assurance)
4. Audit topic 4 (consulting)
5. Audit topic 5 (consulting)
6. Audit topic 6 (assurance)
7. Audit topic 7 (assurance)
8. Audit topic 8 (assurance)
9. Audit topic 9
10. Audit topic 10
11. Audit topic 11
12. Audit topic 12
13. Audit topic 13
14. Audit topic 14
15. Audit topic 15

Internal audit watch list
- Next 6 months
- Later 6 months

Heat Map Key:
- High Risk: Relevant topic is of highest significance, regardless of management effectiveness
- Medium Risk: Relevant topic is of higher significance and moderately or well managed
- Low Risk: Relevant topic is lower significance and well managed

© 2020 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP127086-1A
Incremental steps
Identify audit topics and draft plan (continued)

Some steps to consider:
- Change nature of audit efforts
- Shorten duration of plan

Plan segments
- Regulatory and compliance
- Operational and other recurring or cyclical work
- Risk based, nonrecurring
- Emerging risk, nonrecurring
- Consulting support and requests

Engagement nature
- Assurance
- Preassurance: Preimplementation and readiness assessments
- Consulting: Maturity assessment, investigations, and special requests

Plan duration
- Multiyear
- Annual
- Semiannual or other periodic
- Continuous
- As needed
CPE question

Which option best describes the current duration of your IA plan?

A. Multiyear view
B. Full, one-year view
C. Six-month focus with full-year outlook
D. Quarterly focus, with possible further outlook
E. Shorter than quarterly
Approve and execute plan

Incremental steps

Some steps to consider:
— Utilize alternative resourcing

Best for recurring needs
Things to consider in hiring:
Foster relationships with key universities
Source nontraditional backgrounds (e.g., STEM)
Redesign talent acquisition strategy for digital natives
Redefine employee value proposition to retain millennial generation

Best for emerging needs
Things to consider in developing:
Invest in career path design, learning, and development
Reskill workforce to deliver more business-centric services
Redefine role definitions and core competencies
Develop succession plan to address the retiring and incoming workforce

Best for specialist and extended needs
Incorporate a flexible workforce into the organizational structure
Develop a multifaceted workplace ecosystem (e.g., onshore and nearshore)
Partner to build capabilities that feed into an environment of high-performing talent
Bringing it all together to optimize
Seeing this in action: Risk profile view

Risk profile

Using a visualization tool like Tableau provides a summary view of risk trends by domain, highlighting quantitative and qualitative factors.

A more detailed view is created below, displaying auditable entity level risk across all domains.
Seeing this in action: Quantitative metrics by risk domain

Quantitative metrics

Through analytics and visualization, we can connect a variety of internal or external, quantitative data points specific to each risk domain.

This example is for People and talent risks, with Employee surveys and Employee turnover metrics as risk indicators.
Seeing this in action: Qualitative/ survey insights

Qualitative insights

Surveys or questionnaires are a way to bring in qualitative insights alongside quantitative metrics. These insights can be collected at a variety of points in the process and aggregated by group.
Identification of audit topics
Once qualitative inputs have been layered in, a prioritized view of audit topics allows for a conversation on risk response. Ultimately this drives the audit plan and effective collaboration across lines of defense.
Seeing this in action: Finalizing the audit plan

Audit plan management

Once audit plan topics are identified, resourcing and level of effort, amongst other factors, are considered to build the plan for review and approval.
CPE questions

To what extent does your risk assessment process use data-driven risk insights?

A. Limited qualitative and manual

B. Expanded qualitative and manual

C. Qualitative and limited quantitative; partial tech. enabled

D. Quantitative and expanded qualitative; tech. enabled

E. Balanced quantitative and qualitative; tech. enabled
Final thoughts and Q&A
Final thoughts

**Our vision:** Risk assessment and IA planning that is proactive, data driven, and dynamic

**Guiding principles to achieve this vision:**
1. Mindset and **strategy** shift from defensive to proactive
2. **Deeper insights** are incorporated through use of data analytics and technology.
3. **Risk** is more frequently assessed.
4. Continuous **risk monitoring** and sensing capabilities are in place.
5. **IA plan** is adaptive to changes in the risk landscape.
6. **Alignment** with other risk functions
CPE questions

Which guiding principle is most critical to act on right away?

A. Mindset and strategy shift from defensive to proactive
B. Deeper insights incorporated through data analytics and technology
C. Risk is more frequently assessed
D. Continuous risk monitoring and sensing capabilities in place
E. IA plan is adaptive to changes in the risk landscape
Thank you

Visit us here: http://read.kpmg.us/iar
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.
Appendix
Related resources

**KPMG resources**

**Webcast on November 12, 2020:** An Economic Update with KPMG Chief Economist Constance Hunter
Register here

**White paper:** Identify emerging risks before it’s too late
Available here

**White paper:** Insights to take you forward; Financial Services IT Internal audit priorities for 2020
Available here

**Video:** Continuous risk assessment
Available here

**The IIA resources**

**Internal Auditor November 2020:** “Adapting to the Dynamic Risk Environment”
Available here

**The IIA OnRisk 2021 Report**
Available here

**The IIA OnRisk 2020 Report**
Available here

**The IIA Practice Guide:** Developing a Risk-based Internal Audit Plan
Available here
**Existing standards and guidance**

**IIA Standards**
- 1210 Proficiency, 1220 Due professional care
- 2010 Planning: The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization’s goals. Risk assessment is performed at least annually, includes input of senior management and the board, and is documented.
- 2020 Communication and approval: CAE communicates plan and resource requirements, including any significant changes, to senior management and the board for review and approval.

**COSO**
- Internal Control – Integrated Framework
- Enterprise Risk Management – Integrating Strategy and Performance

**Federal Reserve Board SR13-01**
- Supplemental guidance section 2 – C: Audit universe, Internal audit risk assessment, Internal audit plan, Internal audit continuous monitoring

**Office of the Comptroller of the Currency**
- Comptrollers Handbook – The covered bank’s risk management framework complies with the Guidelines and is appropriate for the size, complexity, and risk profile of the covered bank.

**Additional IIA guidance**
- IIA Practice Aid: Developing a Risk-based Internal Audit Plan
- IIA On Risk 2021 and 2020
Incremental steps

Larger example: Risk universe

- Risk universe
  - Incremental steps
  - People and talent
    - Workforce and talent management
    - Compensation and benefits
    - Training and development
  - Financial
    - Capital management
    - Business continuity
    - Corporate governance
  - Legal/compliance
    - Health and safety
    - Environmental and sustainability
    - Legal, regulatory, and investor compliance
    - Internal controls over financial reporting
  - Technology and data
    - Financial reporting
    - Treasury management: cash, liquidity, and debt
    - Budgeting, forecasting, and financial trending
    - M&A strategy
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management
  - Strategic
    - Reputation and public relations
    - Code of conduct and ethics
    - Fraud and unauthorized acts
  - Cultural
    - Alignment and monitoring of strategic initiatives
    - Organizational performance management
  - Financial
    - Talent recruiting and retention
    - Performance management
    - Succession planning
  - Technology and data
    - Conflicts of interest
    - Leadership and decision-making
    - Public service accountability
  - Operational
    - Customer and sales operations
    - Suppliers, vendors, and third parties
    - Production operations and inventory management

Consideration of strategic risks is key to acting proactively and increasing focus on disruptive risks.

Risks occur in clusters and rarely stand alone.
In incremental steps

Larger example: Audit efforts and plan duration

Possible output – illustrative only

Top Audit Plan topics by Risk Ranking

Heat Map Key

High Risk

Relevant topic is of highest significance, regardless of management effectiveness.

Medium Risk

Relevant topic is of higher significance and moderately or well managed.

Low Risk

Relevant topic is of lower significance and well managed.

Proposed audit projects
Next six months

1. Audit topic 3 (assurance)
2. Audit topic 4 (consulting)
3. Audit topic 5 (consulting)
4. Audit topic 6 (assurance)
5. Audit topic 7 (assurance)
6. Audit topic 8 (assurance)
7. Audit topic 9 (assurance)
8. Audit topic 10 (consulting)
9. Audit topic 11 (assurance)
10. Audit topic 12 (consulting)
11. Audit topic 13 (consulting)
12. Audit topic 14 (assurance)
13. Audit topic 15 (assurance)
14. Audit topic 3 (assurance)
15. Audit topic 4 (consulting)

Internal audit watch list
Later 6 months

1. Audit topic 9
2. Audit topic 11
3. Audit topic 12
4. Audit topic 13
5. Audit topic 14
6. Audit topic 15
7. Audit topic 9
8. Audit topic 11
9. Audit topic 12
10. Audit topic 13
11. Audit topic 14
12. Audit topic 15
13. Audit topic 3 (assurance)
14. Audit topic 4 (consulting)
15. Audit topic 5 (consulting)

Status of risk management (current vs. desired state)

Significance (impact, velocity, likelihood)

Well managed
Mostly managed
Moderately managed
Loosely managed
Non-existent

New auditable entity

© 2020 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. NDP127066-1A