The internal audit risk assessment and integrated audit plan

Milwaukee IIA

30 August 2018
What is an integrated audit?

An integrated audit considers information technology, financial and operational controls as mutually dependent for establishing an effective and efficient internal control environment. ... The integrated audit includes an audit of the applications, servers, and network configurations that support the business process. ~ Harvard University
Internal Audit Operating Framework

Drivers
- Governance
- People
- Infrastructure and Operations

Building blocks
- Purpose and mandate
- Competency development
- Resource
- Sustaining people excellence
- Tools and technology
- Knowledge management
- Operations
- Quality
- Continuous improvement and change management

Impacts
- Audit Committee, charter and governance arrangements
- Structure
- Resourcing, training, and compliance
- Stakeholder management
- Planning/targeting
- Audit Execution
- Methodology
- Reporting, escalation and follow-up
- AS1000 – Purpose, authority, and responsibility
- AS1100 – Independence and objectivity
- AS1130 – Impairment to Independence and Objectivity
- AS1200 – Proficiency and due professional care
- PS2100 – Nature of work
- PS2600 – Communicating the acceptance of risk
- AS1300 – Quality assurance and improvement plan (QAIP)
- PS2000 – Managing the IA activity
- PS2200 – Engagement planning
- PS2300 – Performing the engagement
- PS2400 – Communicating results
- PS2500 – Monitor progress

IIA Code of Ethics and International Standards for Internal Auditing
Key Trends in IA

► Introduction to dynamic risk assessment:
  ► Move from develop, present, and defend to collaborate and team with stakeholders (audit committee, senior leadership, and process owners)
  ► Iterative risk planning process vs. annual risk assessment
  ► Incorporate various risk functions (e.g., ERM, SOX, legal, IT)
  ► Apply advanced data analytics to provide additional layers of risk analysis

► Shift from compliance to strategic:
  ► Align with strategic and business objectives
  ► Drive efficiencies and add value to the business
  ► High level of collaboration with business units
  ► Focus on emerging risks
  ► Categorize as preventable, external, and strategic
  ► Assess impact of velocity, volatility, and visibility of risks
Key Trends in IA

► Increased usage technology to achieve plan:
  ► Analytics
  ► Block chain
  ► RPA
  ► AI and connected technologies
  ► Process mining

► Improvement in value charter including:
  ► Movement from internal metrics to those focused on all stakeholders
  ► Qualitative aspects of internal audit activities (e.g., communication and relationship building)
IA Trends – Honorable Mention

- The need to do more with less – managing the cost of compliance
- Rotational programs to promote skill diversification – one dimensional skill sets
- Increased “partnering” with stakeholders on special projects – seat at the table
Companies typically manage risks across three key lines of defense.

Risk Management = minimize deviation from expected outcomes (both positive and negative) due to uncertainty in actions and events.

---

**Business Strategy**
- **Strategic**
  - Drive increased pipeline; R&D productivity
- **Operations**
  - Growth: organic and inorganic, developed and emerging markets
  - Expand margin, optimize cost, streamline supply chain
- **Financial**
  - Asset and capital management

**Executive Management**
- **Compliance**

---

**Risk Functions**
- Research & Discovery
- Clinical Development
- Procurement
- Manufacturing & Supply Chain
- Sales & Marketing
- Post Marketing

**Support Functions**
- Transactions
- IT
- Tax
- Finance
- Legal
- HR

---

**Risk Management**
- Internal Controls
- IT Compliance
- Mfg. Quality
- Legal & Regulatory
- Others

**Operations and Business Units**
- First Line of Defense
- Second Line
- Third Line

**Achieve Business Objectives**
- Executive Management
  - Board
  - Audit Committee
  - Risk Committee

**Make Our Business Better**

**Keep Us Out of Trouble**

---

**COORDINATED APPROACH TO RISK**
- Coverage
- Oversight

---

**Companies typically manage risks across three key lines of defense**

---

Page 8
Assurance and/or advisory

► As stakeholders demand more, IA needs to align its focus to these expectations. Focus will be balanced not just on the assurance activities historically incorporated in audit plans, but also to continue to increase advisory activities that drive business insights and serve as a source of independent advice.

► Finding that balance is unique to each organization and its strategic objectives.

► This balance does not become stagnant, but continually teeters between the two as objectives change.

Internal Audit needs to be nimble and flexible in order to respond to the changing environment.

Split between Assurance and Advisory Reviews

<table>
<thead>
<tr>
<th>ENTITY Current State</th>
<th>Leading Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Assurance</td>
</tr>
<tr>
<td>95%</td>
<td>5%</td>
</tr>
</tbody>
</table>
Internal Audit’s advisory role

**Leading practice**

- Internal Audit (IA) is moving to an assurance/advisory role that enables it to assess the effectiveness, efficiency and reliability of the organization’s risk management program.
- IA will continue to be expected to fulfill compliance mandates while also providing business insights and acting as strategic advisor to the business, all while maintaining or reducing costs.
- As a result, IA can determine the extent to which it can leverage the work of others.
- IA can now focus more of its efforts on the risks that matter, including strategic risks.

84% of respondents say risk management oversight is provided by someone other than Internal audit.

43% of respondents say Internal Audit leverages the work of others today.

75% of respondents say Internal Audit will leverage the work of others in 3 years.

Leading practices demonstrate that the percentage of advisory reviews to the total audit plan hours ranges from 15%–35%.

Source: EY survey
Assurance and advisory reviews are undertaken by IA with a view to providing an objective and independent assessment of governance, risk management and control processes.

- Compliance with policies and procedures
- Adequacy of the design of internal control
- Operating effectiveness of internal controls

Advisory reviews are designed to be preventive in nature by focusing on the upstream design and implementation of strategies, business processes and systems.

- Control-design consulting
- Benchmarking analyses
- Process improvement
- Pre/post system implementation
- Controls training

Issue-level rating is provided for assurance reviews:

- Issue-level rating is provided for assurance reviews
- Engagement-level rating is provided at the conclusion of assurance reviews
- Deliverable in the form of a formal report (findings and recommendations)
- Resolution of issues will be followed up upon accordingly

Formal ratings are typically not assigned to advisory reviews:

- Formal ratings are typically not assigned to advisory reviews
- Deliverables vary depending on type of review and are in the form of an advisory report or memo outlining observations and recommendations related to:
  - Process diagrams and controls matrices
  - Gap analysis
  - Leading practice recommendations
  - Observations that have a critical impact on risk will be followed up upon

An appropriate balance between assurance and advisory is required so that advisory services, while helpful, do not prevent IA from fulfilling its fundamental assurance role.

Maintaining the overall balance between assurance and advisory reviews can be achieved through the following:

- Identifying key management initiatives aligned with organizational strategy as potential advisory projects
- Scope assurance reviews to identify specific and measurable opportunities to gain efficiencies

Leading practices demonstrate that the percentage of advisory reviews to the total audit plan hours ranges from 15%–35%.
Survey Responses
IA risk assessment survey responses

Timing

Do you perform a risk assessment more than annually?

- No
- Yes
IA risk assessment survey responses

Process

What inputs do you use in your risk assessment process?

- Analysis of financial results
- Industry trends
- Analysis of competitor or peer risks
- Past external audit issues
- Past internal audit or SOX issues
- ERM Assessment
- Surveys
- Interviews
- Other

Do you leverage 3rd party external risk data as part of your risk assessment process?

- No
- Yes

If you interview or survey, who is involved in providing input?

- Other
- External Auditor
- BU Leaders
- CIO/CTO
- CFO
- CEO/COO
- Audit Committee Chair

Who do you involve in conducting the risk assessment?

- Third parties
- Subject matter resources
- All levels within the department
- IA Managers or higher
IA risk assessment survey responses
Data analytics

To what degree do you leverage data analytics in your assessment process?

- I do not leverage analytics
- High
- Moderate
- Low

How do you see the use of data analytics in your risk assessment and audit planning process changing in the future?

- Decreasing
- Staying the same
- Increasing

What is your biggest challenge to leveraging data analytics in the risk assessment process?

- Difficulty identifying and collecting data
- Lack of people with the appropriate knowledge and experience
- Lack of access to tools
IA risk assessment survey responses
Interview/survey techniques

How many surveys do you conduct as part of your risk assessment?

- More than 60
- 40 – 60
- 20 – 40
- 1 - 20
- 0

How many interviews do you conduct as part of your risk assessment?

- More than 30
- 20 - 30
- 1 - 20
- 0

What tools do you leverage in your risk assessment process?

- Automated Surveys
- Computer aided group interviews
- Polling tools
- Other
IA risk assessment survey responses
Collaboration with other lines of defense

**Is your Internal Audit risk assessment also leveraged as the Company’s ERM assessment?**
- No
- Yes

**How would you describe integration with other risk assessment activities occurring at your company?**
- NA
- Low
- Moderate
- High

**What functional groups do you collaborate with in conducting your risk assessment?**
- N/A
- Other
- SOX group
- Compliance
- IT Security
- ERM function
## IA risk assessment survey responses
### Audit plan creation and validation

### What inputs do you use to prioritize audits on your plan (check all that apply)?

<table>
<thead>
<tr>
<th>Input</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>An ideal mix of audits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk universe coverage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Value to the organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relevance to strategic objectives</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Competencies available in IA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last time audited and audit results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Velocity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk impact / likelihood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Who do you validate your internal audit plan with?

<table>
<thead>
<tr>
<th>Validator</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BU Leaders</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIO/CTO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CEO/COO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CFO</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit committee/board</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### How do you describe your internal audit plan (check all that apply)?

<table>
<thead>
<tr>
<th>Description</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic internal audit plan that changes throughout the year and is reset at selected milestones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heavy focus on SOX and geared towards reliance by the External Auditor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heavy rotational plan that provides coverage of the business over time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk-based plan that closely ties to the top enterprise risks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Do you prioritize based on a set mix of audits (e.g. financial vs. compliance vs. operational)?

<table>
<thead>
<tr>
<th>Option</th>
<th>0</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>12</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Trends in Risk Assessments
Why is the need for a world-class internal audit risk assessment more vital than ever?

There are multiple drivers behind the growing importance and need to execute a robust and comprehensive risk assessment:

The velocity of change is at an all time high

- Business models and strategies are evolving at an unprecedented pace
- Significant M&A activity
- Organizations today have a greater dependency on 3rd parties
- Volatile currencies / significant activity focused on emerging markets and developing countries
- Increased regulatory demands / significant accounting changes
- Increased dependency on new and unfamiliar technologies

Too much information rather than a lack of it has become the problem – companies need to determine the signal from the noise and audit the risks that matter most!
Risk assessment process

- Identify Risks to Company
- Assess Risks within potential scope of IA
- Prioritize Risks within potential IA Scope
- Results from Risk Assessment
- Management Expectations
- Achievement of Compliance Objectives

- Market Data – Emerging Risks
- Historical Audit Data
- Stakeholder Input
- Internal Financial Data
- Regulatory Information
- Collaboration Data

Company mgmt. separately addresses risk outside of context of Internal Audit

Align risk to recommended audit effort and approach

- Internal Audit Plan
## Risk assessment leading practices

### Basic vs. leading practice risk assessment techniques

<table>
<thead>
<tr>
<th>Components</th>
<th>Basic (lower degree of confidence)</th>
<th>Leading (higher degree of confidence)</th>
</tr>
</thead>
</table>
| **Data reviewed** | ► Internal audit issues  
► SOX and external audit issues  
► Last time audited a process | ► Root causes and trend analysis  
► Turnover of key personnel  
► Footprint vs. corruption perception index / fraud hotline calls  
► Competitor and peer risks/ 10k reviews  
► Industry mega trends  
► Analyst reports |
| **Data analytics** | ► Analytics run but limited summarization of data  
► Business and IA leadership struggle to spot trends in data | ► Trending and period-to-period comparisons to identify emerging risks or unexpected changes  
► After determining the “what” ;analytics can help you determine the “where” to audit – help find the needle in a haystack |
| **Stakeholder engagement and Interviews** | ► Only focus on top Finance/Accounting/IT stakeholders  
► Heavy emphasis on “home office” stakeholders only  
► Point-in-time engagement primarily during annual risk assessment  
► Interviews done via a phone call with canned questions | ► Includes operational and global stakeholders beyond Finance/Accounting/IT  
► Comparison of executive themes and prioritizations with the comments made by line management  
► Continuous dialogue with stakeholders (monthly, quarterly meetings) to identify changing priorities for audit- leading to an efficient “rolling risk assessment”  
► Includes external auditors  
► All interviews done face to face and one at a time  
► Ask the hard questions |
Risk assessment leading practices
Basic vs. leading practice risk assessment techniques

<table>
<thead>
<tr>
<th>Components</th>
<th>Basic (lower degree of confidence)</th>
<th>Leading (higher degree of confidence)</th>
</tr>
</thead>
</table>
| Interview/ survey techniques  | ► Inconsistent documentation of interviews  
► Leading questions / same questions  
► Surveys only used for SOX 302 certification purposes or not at all  
► Ask “what keeps you up at night”                                                                 | ► IT and other subject-matter resources participate in select interviews to draw out key risks  
► Interview questions are flexed to be fully relevant to the interviewee  
► Solicit feedback regarding components outside of the interviewee’s area of responsibility  
► Surveys used to confirm risk assessment results with lower-level management not interviewed |
| Collaboration                 | ► Internal audit attends interviews with little participation from other risk management functions or operational audit | ► Risk assessment collaboratively developed and leveraged by internal audit and other risk management functions  
► SOX, external audit and other risk management functions participate in interviews if separate functions exist  
► Aligned to ERM and other risk management offices (security, compliance etc.) |
| Audit prioritization          | ► Impact and likelihood utilized for prioritization  
► Audits prioritization based heavily on competencies available in IA department  
► Audit priorities are based solely on last time audited/ rotation                                                                 | ► Relevance to strategic objectives is utilized to prioritize risks  
► Audits executed based on value to organization and connection to strategic objectives  
► Audits vary in length and priority/ how audits are completed and risks are monitored is flexible  
► The audit plan stretches capabilities to truly address the risks that matter |


Emerging risks to consider in your internal audit plan

► Business continuity
► **Cloud technologies**
► Commodities
► Construction management
► Corporate culture
► **Cybersecurity (IoT, operational technology)**
► Data privacy
► Derivatives and hedging
► Financial metrics and monitoring
► Fraud and corruption
► General Data Protection Regulation (GDPR)
► Identify and access management
► IT risk management
► Large capital programs
► Lease accounting
► Marketing and sales channel effectiveness
► **Mergers, divestitures and acquisitions**
► Mobile device security
► Nonfinancial reporting
► Organization performance (metrics)
► Real estate contract reviews
► **Reputational risk and crisis management**
► Revenue recognition
► Robotics process automation (RPA)
► Social media
► Supply chain
► Talent management
► Tax
► **Third-party risk management**
► Treasury
External risks to consider

In laying out your business strategy, have you effectively consider external risks in the short and long-term?

Sources of external risks

**Political**
- Shareholder and external activism
- Uncertain political leadership (national and international)
- Geopolitical shifts and political instability
- Continuing conflicts and terrorism

**Cybersecurity**
- Business transformation (technology dependence)
- New and evolving technologies
- Digital nature of data
- Sophistication of hackers

**Social**
- Business and governance corruption
- Public health
- Social unrest and stratification
- Recruitment and retention

**Technological**
- Social media
- Mobile connectivity
- Cloud computing
- Data analytics

**Legal**
- Expansion of governments role
- Privacy risks and cyber attacks
- Regulation and compliance
- Changes in tax law

**Economic**
- Competitive pricing and profit pressure
- Macroeconomic risks and related market volatility
- Increasing role of government as a market actor
- Sovereign debt default

**Environment**
- Sustainability
- Maturing markets
- Climate change
- Natural resource management
### Types of projects

#### Audit planning

The Response Continuum (RC) is a mechanism to consider and formally articulate Internal Audit’s options to address risk and controls, particularly at the high risk level. Techniques range from verbal audit responses (e.g., giving advice at steering committee meetings) to business education, to substantial audits. The responses are not mutually exclusive; often teams use a combination. However, they allow Internal Audit to make explicit decisions on how it can add the most value and be most efficient with resources.

The response “menu” is a robust Internal Audit planning process. The audit approach selection is explicitly based on: the complexity and nature of the risk and controls being audited; the objectives of the organization and the degree of assurance required; and the skills required. The flexibility and proportional response provides for:

- A more sophisticated and broad approach to planning and delivering Internal Audit engagements;
- Clearer alternatives in selecting the most appropriate response;
- Explicit audit planning decision making;
- Better language in discussions with the stakeholder/auditee; and
- More transparent reporting of effort.

<table>
<thead>
<tr>
<th>Response category</th>
<th>Response</th>
<th>Current State</th>
<th>Future State</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard reviews</strong></td>
<td>1 Health check/diagnostic</td>
<td>95%–100%</td>
<td>50%–60%</td>
</tr>
<tr>
<td></td>
<td>2 Standard sample testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3 Project/engagement monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 Pre-implementation review</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5 Post-implementation review</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 Compliance audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Complex reviews</strong></td>
<td>7 End-to-end process audit</td>
<td>0%–5%</td>
<td>20%–30%</td>
</tr>
<tr>
<td></td>
<td>8 Deep dive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>9 Investigation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 Rapid assessments and diligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Risk and control reviews</strong></td>
<td>11 Risk monitoring</td>
<td>0%</td>
<td>10%–20%</td>
</tr>
<tr>
<td></td>
<td>12 Project management monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>13 Control monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14 Control framework review</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>15 Business coaching/education</td>
<td>0%</td>
<td>5%–10%</td>
</tr>
</tbody>
</table>
Guidance on when to use ‘Standard audits’

Health check/diagnostic
► Assess the control environment when management is considering a change in business processes or responsibilities.
► Assess whether an identified issue is systemic.

Compliance audit
► Provide comfort that contractual or regulatory obligations are being met.
► Help management determine compliance with contractual obligations or industry best practice.

Pre-implementation review
► Provide comfort on a major transaction or project before it goes live, including:
  ► Assess implementation and communications plans
  ► Review key documentation
  ► Review risk/project status reporting
  ► Assess data conversion and migration strategies
  ► Review data cleansing process
  ► Test user acceptance
  ► Interview key participants
  ► Assess stakeholder buy-in

Post-implementation review
► Assess the live control environment to ensure it is operating as intended.
► Include more substantive audit procedures, as benefit realization.

‘Standard’ sample testing
► Test key controls to confirm their design and operating effectiveness, using data analytics, transactional testing, root cause analysis.
► High level, not deep dive.

Project/Engagement monitoring
► Evaluate governance framework for robustness.
► Assess the likelihood of the project realizing intended benefits.
► Review key dimensions of the risk management program to confirm it is sufficient.

Standard audits
Common reviews performed by Internal Audit using a relatively standard work program.
Guidance on when to use ‘Complex reviews’

<table>
<thead>
<tr>
<th>Complex reviews</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use to provide in-depth, value-added service</td>
</tr>
</tbody>
</table>

**End-to-end process audit/thematic review**
- Evaluate a core process impacting multiple business units, geographies and/or reporting periods. Used by global enterprises, where integrated processes cut across many locations.
- Audit activities focus on how the process is managed across different areas, focusing on process inter-dependencies and hand-over controls and considering some or all of the following:
  - Beginning-to-end process flows
  - Process inputs and outputs
  - Key performance indicators
  - Critical success factors
  - Dependencies between business units or geographies
  - Process efficiencies

**Deep dive**
- Provide a more in-depth level of comfort over both operational and IT controls, including the underlying data.
- Focus on risks and controls at a granular level, with substantive transactional testing, increased sample sizes and more extensive testing procedures.

**Investigation**
- Conduct an investigation for improper conduct, fraud or unethical behavior.
- Procedures are likely to include interviewing key stakeholders and reviewing relevant documentation under the direction of a suitably qualified forensics specialist.
- Significant use of fraud analytics.

**Rapid assessments and diligence**
- Quickly assess risks and assist BUs with defining and prioritizing integration activities for a new acquisition.
  - Develop an inventory of all finance and accounting processes and systems.
  - Compare finance processes and controls to company standards to identify gaps.
  - Identify and assess high risk areas related to financial reporting.
Guidance on when to use ‘Risk & control framework reviews’

**Risk & control framework reviews**
Common reviews performed by Internal Audit to evaluate the effectiveness of the control environment

- **Risk monitoring**
  - Use verbal reviews when management needs ‘real time’ feedback about key risks
  - A preliminary response identifying the need for more in-depth work and should be backed up by a minute, file note or internal memo
  - Quickly and efficiently assess:
    - How management sees risk and its impact on the business
    - Controls implemented to mitigate the identified risks.
    - Whether they believe controls are effective and efficient

- **Control Monitoring**
  - Provide comfort over how a process is functioning at a macro level
  - Focus on a processes’ key risk and controls, using gap analysis to assess the design effectiveness of controls rather than their operational effectiveness
  - Based on a variety of techniques including:
    - Interviewing key stakeholders
    - Documenting process flows
    - Identifying control points
    - Performing walkthroughs
    - Reviewing process related documents

- **Project management monitoring**
  - Monitor actions over the risks around key business objectives by conducting interviews and attending Steering Committee Meetings
  - Depending on the risks and project/initiative requirements, consider:
    - Participating on the Steering Committee
    - Observing risks are being identified and proactively mitigated
    - Conducting in-depth auditing procedures as required

- **Control Framework Review**
  - Review the effectiveness and appropriateness of a control framework, usually by benchmarking against leading practice
  - Consider the balance between effectiveness and efficiency
Thematic audits: consider approach for coverage based on overall organizational strategy and risk profile

Thematic audits: consider approach for coverage based on overall organizational strategy and risk profile

Themes might include …

- **Process or function**
  - Security
  - Human capital
  - Inventory management
  - Cost management
  - Regulatory and compliance
  - Working capital
  - Plant modernization
  - Transaction
  - Interim and internal transformations
  - Cash management
  - Tax

- **Geography**
  - Audit by geography when footprint & market maturity varies significantly by region
    - Strategic options: Is there a regional/national focus?
    - Are services worthy of standardization?
    - How will R&D be managed?
    - How will manufacturing be managed?
    - How will it be managed economically?
    - Are the R&D results leveraged?
    - Can the business be cost effective in other markets?

- **Product or service**
  - Audit by product, thematic areas when product areas are diverse and/or autonomous
    - What are the differences?
    - Can they be leveraged?
    - Are they worthy of standardization?
    - Are they leveraged?

Beneficial when certain processes or functions have a significantly different risk profile

Beneficial for organizations with distinct markets in different stages of growth

Beneficial when there are divergent products, product segments and/or services

Survey insight – stakeholders want to understand what overarching issues exist in the organization.
Issue-based audits: demonstrate IA’s value and relevance by providing insight on strategic business issues

- Mergers, acquisitions and/or divestitures
- Major construction projects and capital programs
- Material contracts
- IT systems implementations
- New market entry
- New product launch
- Cybersecurity

Can be planned or ad hoc and can include a blend of advisory and assurance reviews
## IA advisory opportunities

<table>
<thead>
<tr>
<th>Focus area</th>
<th>Expanded audit services</th>
</tr>
</thead>
</table>
| **Process improvement**          | ► Support major process transformations such as finance, supply chain, customer, etc.  
► Assess processes and identify opportunities for improvement  
► Provide business insights utilizing leading industry practices and specialists' knowledge  
► Providing risk and controls consultation to determine readiness, levels of progress and measurements for success |
| **Business performance management** | ► Support design and documentation of processes to support future state vision and incorporate adequate controls  
► Assist in pre and post implementation review from a controls perspective |
| **Business process outsourcing & SSC** | ► Perform current state risk assessment. Identify risk and readiness for outsourcing if required  
► Support in establishing process and controls around setting up a shared services center  
► Evaluate processes for benefits tracking |
| **Mergers & acquisitions**        | ► Review company’s readiness to go through a merger or acquisition.  
► Alert business of potential risks and monitor associated controls |
| **Technology implementation**     | ► Identify risks to provide controls consultation  
► Participate actively in the Program Management Office |
| **New product development**      | ► Analyze risks and controls to avoid recurring product delays and cost overruns  
► Conduct due diligence and planning prior to development |
| **Expanding footprint**           | ► Review readiness to understand impact on business  
► Share leading practices for successful expansion |