IIA Malaysia e-techline
October 2019 Issue 04/19

DEMONSTRATING THE CORE PRINCIPLES FOR THE PROFESSIONAL PRACTICE OF INTERNAL AUDITING - Enablers and Key Indicators

The IIA's Core Principles for the Professional Practice of Internal Auditing characterise the effectiveness of the internal audit activity. By achieving the Core Principles, the internal audit activity also achieves the Mission of Internal Audit: "to enhance and protect organisational value by providing risk-based and objective assurance, advice, and insight."

1. Core Principle 1: Demonstrates integrity.

Figure 1: Examples of Core Principle 1: Demonstrates integrity.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
▪ The IIA Code of Ethics is referred to in the internal audit charter and built into the QAIP. ▪ The internal policies and/or internal audit training includes ethical scenarios/case studies that are specifically relevant to internal auditors. ▪ The CAE has informed the internal audit activity of their ethical responsibilities. ▪ Training on The IIA Code of Ethics and the organisation's code of conduct/ethics takes place. ▪ Internal auditors have an annual confirmation of compliance with The IIA Code of Ethics and organisation's code of conduct/ethics.	▪ No cases of disciplinary action against internal auditors relating to violations of The IIA Code of Ethics or the organisation's code of conduct/ethics. ▪ Internal audit team member survey results indicate that employees believe the department operates with integrity and that concerns raised by employees will be properly addressed. ▪ Feedback from surveys or interviews from areas under review indicates that team members demonstrate integrity. ▪ Internal audit team has completed ethics-related CPE/CPD requirements.

2. Core Principle 2: Demonstrates competence and due professional care.

Figure 2. Examples of Core Principle 2: Demonstrates competence and due professional care.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
Competence ▪ Internal audit activity structure is defined and supported with job descriptions. ▪ An internal audit activity competency model is accompanied by a staff development programme. ▪ Internal audit activity's annual training plan, linked to development needs, is prepared and executed. ▪ A policy is developed encouraging earning certifications or designations. ▪ Performance management system with key objectives for the internal audit activity is linked to departmental objectives. ▪ Guest auditor procedure/co-sourcing contracts are in place.	**Competence** ▪ Skills required to audit key risk areas of the organisation can be matched to in-house team and/or with co-sourced provider. ▪ Percentage of internal auditors who have undergone 40+ hours of training per annum. ▪ Percentage of internal auditors with above average evaluations in performance appraisals. ▪ Percentage of team who have earned certifications or designations.
Due Professional Care ▪ Audit risk is actively addressed in the QAIP. ▪ Internal auditors complete sufficient background research as part of engagement planning to have informed discussions with the audit client. ▪ Supervision and review of engagement level work programme and activities is conducted by appropriately skilled individuals. ▪ The performances of the internal audit activity is assessed after each engagement. ▪ Assurance procedures change based on the level of engagement risk.	**Due Professional Care** ▪ Limited or no disagreements with audit client after final reports issued. ▪ No cases of major errors or omissions in reports are identified after final reports are issued. ▪ Percentage of internal audit management oversight and review of audit engagements compared to total hours. ▪ No instances of internal audit activity failing to escalate delayed closure of high-risk audit observations.

3. Core Principle 3: Is objective and free from undue influence.

Figure 3. Examples of Core Principle 3: Is objective and free from undue influence.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
Objectivity ▪ Confirmation of objectivity is submitted annually to the board. ▪ Process exists to verify whether 3rd party assurance providers have performed work for management that constitutes a conflict of interest. ▪ Internal auditors do not provide assurance over areas for which they had responsibility within the previous 12 months. ▪ Internal audit recommendations are clear, factual, reliable, and relevant.	**Objectivity** ▪ Feedback from audit client surveys or interviews indicating internal auditors appear impartial and objective. ▪ Internal auditors have completed forms acknowledging they are free from conflicts of interest or disclosing any potential conflicts. ▪ Assessment as part of the internal audit activity's QAIP affirm that conclusions and opinions were arrived at objectively.
Independence/Freedom from Undue Influence ▪ Functional reporting to the board is defined in the internal audit charter. ▪ Board/audit committee formally reviews CAE's independence and objectivity on a periodic basis in relation to ongoing employment. ▪ The CAE has direct access to the board as defined in the internal audit charter.	**Independence/Freedom from Undue Influence** ▪ Board reviews CAE performance and approves appointment, compensation, and termination. ▪ Low number of inhibitors/restrictions to the scope of work that the internal audit department has experienced. ▪ Regularly scheduled private sessions with board without the management present.

4. Core Principle 4: Aligns with the strategies, objectives, and risks of the organisation.

Figure 4. Examples of Core Principle 4: Aligns with the strategies, objectives, and risks of the organisation.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
Objectivity ▪ The internal audit activity's strategic plan, aligned to the organisational strategy, is developed with a defined vision, objectives, and clear measures of success. ▪ The internal audit activity's audit strategy is updated based on changes to the internal or external environment. ▪ The internal audit activity's annual audit plan is updated based on changes in the organisation's strategies and/or objectives. ▪ Internal audit plan links engagements to a strategic objective (s) and/or risk(s). ▪ Top organisational risks are used as the basis of the annual plan. Top risks not addressed in the internal audit plan are communicated to the board.	**Objectivity** ▪ Feedback from stakeholder surveys indicates that the internal audit activity is operating in alignment with stakeholders' view of priorities. ▪ CAE attends strategy discussions. ▪ Percentage of internal audit plan covering strategic projects and/or initiatives. ▪ Strategic risks are identified in the internal audit plan. ▪ Strategic planning has been audited. ▪ Percentage of internal audit staff skilled and assigned in alignment with the organisation's structure and key risks.

5. Core Principle 5: Is appropriately positioned and adequately resourced.

Figure 5. Examples of Core Principle 5: Is appropriately positioned and adequately resourced.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
Appropriately Positioned ▪ A documented and customised internal audit charter, aligned with the IPPF, is in place. ▪ Functional reporting to the board level and administrative reporting to the highest level in the organisation is defined in the charter. ▪ Internal audit activity's mandate is broad and aligned to organisational needs.	**Appropriately Positioned** ▪ CAE is viewed as part of leadership and participates at key management, board, project management, and functional leadership meetings. ▪ Evidence the CAE has challenged management when needed. ▪ Audit engagement results are given due considerations.
Resourcing ▪ A sufficient operating budget is approved by the board. ▪ Periodic discussions occur with the board on QAIP, resource availability, and any limitations. ▪ Periodic benchmarking of resources is compared to similar size/profile organisations. ▪ Human resources, technology, and tools are provided to internal audit enabling them to execute their engagements effectively and efficiently. ▪ The internal audit activity has appropriate access to subject matter specialists through in-house roles, guest auditor programmes, and/or co-source arrangements.	**Resourcing** ▪ Percentage of completion of internal audit plan. ▪ Percentage of internal audits dropped from the internal audit plan due to resource limitations. ▪ Percentage of internal audit plan available for management requests. ▪ Percentage of internal audit hours allocated to core internal audits versus administrative activities. ▪ Percentage of internal audit plan coverage dedicated to high-risk processes and entities.

6. Core Principle 6: Demonstrates quality and continuous improvement.

Figure 6. Examples of Core Principle 6: Demonstrates quality and continuous improvement.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
▪ QAIP elements are operational. ▪ QAIP action items are tracked and closed out on a timely basis. ▪ Mechanisms are in place to solicit feedback from audit clients and key stakeholders. ▪ Operational KPIs are defined and monitored, including KPIs to promote internal audit activity improvements and innovations. ▪ A fit for purpose internal audit methodology is in place and is refreshed periodically. ▪ Outsourced internal audit activities are required to conform with The IIA's *Standards* and Code of Ethics.	▪ Internal assessments include ongoing monitoring of internal audit performance and periodic self-assessments or assessments by others within the organisation sufficiently knowledgeable about internal auditing and the IPPF. ▪ External assessments occur at least once every 5 years and results indicate "general conformance" with IIA *Standards* and Code of Ethics. ▪ Internal and external assessments indicate overall improvement as compared to prior assessments. ▪ Senior management and the board receive the results of the QAIP. ▪ Internal audit activity has an action plan and addresses/closes QAIP action items timely.

7. Core Principle 7: Communicates effectively.

Figure 7. Examples of Core Principle 7: Communicates effectively.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
▪ An internal audit communication plan is in place. ▪ Periodic reporting and some engagement reports are customised for key stakeholders as needed. ▪ Engagement reports are factually accurate, highlight risk, address root causes, and encourage action from management responsible for the area or process under review. ▪ Engagement reports are succinct, aligned with key risks, and use graphics or visuals where appropriate.	▪ Feedback from audit clients and key stakeholders indicates that internal audit reports are fit for purpose. ▪ No cases of major errors or omissions in reports are identified after final reports are issued. ▪ Percentage of planned awareness sessions, social media/intranet posts, etc., completed by internal audit. ▪ No cases of unauthorised or erroneous disclosure of confidential data by internal auditors.

8. Core Principle 8: Communicates effectively.

Figure 8. Examples of Core Principle 8: Communicates effectively.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
▪ Internal audit mandate includes assurance that key risks are being managed or that action plans are in place to address those risks. ▪ Internal audit planning is aligned with top organisational risk universe and risk appetite. ▪ CAE discusses with senior management and the board the provision of assurance over key risks not covered by the internal audit activity. ▪ Internal audit plan is flexible and adapts to changing risks.	▪ Percentage of highly significant risks covered by internal audit plan. ▪ Percentage of emerging risks identified by the business that are included in the internal audit plan. ▪ Percentage of internal audit observations that can be linked back to significant organisational risk. ▪ Engagement-level risk assessment demonstrates that each individual engagement is targeted to identify and test the effectiveness of controls that address the most important risks.

8. Core Principle 9: Is insightful, proactive, and future-focused.

Figure 9. Examples of Core Principle 9: Is insightful, proactive, and future-focused.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
▪ Internal auditors obtain training and education about emerging issues, data analytics, and technology. ▪ CAE maintains a multiyear strategy/strategic plan for the internal audit activity; aligned to the organisational strategy, and developed with a defined vision, objectives, and clear measures of success; and updates regularly. ▪ A structure exists to encourage active, two-way communication with stakeholders. ▪ Systematic issues and/or trends in risk or controls are identified.	▪ Feedback from board and management surveys or interviews indicates that internal audit activity is insightful, proactive, and future-focused. ▪ Percentage of engagements where technology and/or data analytics are used. ▪ Percentage of previously unknown issues/risks identified per engagement. ▪ Percentage of audit observations with forward-looking analysis and issues framing.

10. Core Principle 10: Promotes organisational improvement.

Figure 10. Examples of Core Principle 10: Promotes organisational improvement.

Enablers	Key Indicators
What should be done to operationalise this principle?	**How do we know that we've been successful?**
▪ Internal audit's work programmes make recommendations to improve the organisation's governance. ▪ Closure of audit observations is carefully tracked, validated, and escalated based on risk. ▪ Appropriate coordination takes place with other assurance providers to streamline assurance activities across the three lines of defense. ▪ Best practices, insights, and control/risk trends are shared with the business and across business units.	▪ Percentage of consulting engagements included in internal audit plan. ▪ Number of best practices shared with the business are implemented. ▪ Key stakeholders perceive internal audit to be a business partner and advisor who helps management achieve its objectives in a controlled manner. ▪ Cost savings achieved/identified.

What CAE should do?

- To embrace and demonstrates the Core Principles for the Professional Practice of Internal Auditing to conform with the Mandatory Guidance of the IPPF.

Reference:

https://global.theiia.org/standards-guidance/Member%20Documents/PG-Demonstrating-the-Core Principles-for-the-Professional-Practice-of-IA.pdf

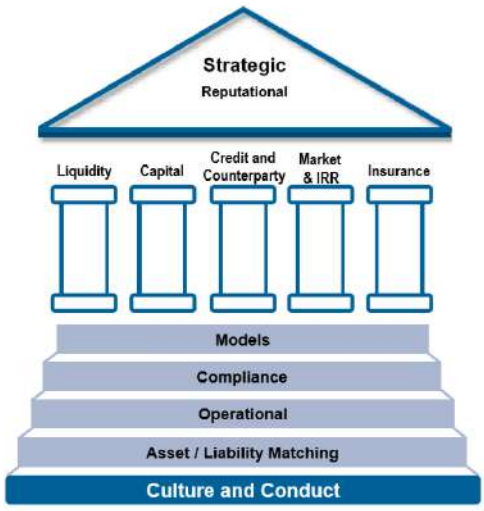
FOUNDATIONS OF INTERNAL AUDITING IN FINANCIAL SERVICES FIRMS

Without appropriate guidance, training, and education, and a code of ethics by which to abide, the financial services industry may be challenged to find enough capable, competent internal auditors to fulfill the responsibilities across this unique landscape. This may lead to unidentified and unmitigated risks, which may increase the risk exposure of financial services firms, increase regulator enforcement actions, and erode consumer confidence.

Managing the internal audit activity properly and with a forward-looking view in this field of high expectations is key. The importance of managing an effective internal audit activity within the financial services industry includes the following:

- The risk landscape in financial services.
- The regulatory landscape in financial services.
- Key principles of sound risk governance.
- Collaboration with other assurance providers.
- Internal audit coverage.
- Internal audit activity management in the context of financial services.

Figure 5: The IIA's Financial Services Risk Framework



Source: The Institute of Internal Auditors.

What CAE should do?

- To understand and identify the following:
  - the financial sector environment, including kehy objectives, business areas, and related risks and the impact of globally accepted principles that provide the foundation for laws and regulations within the industry;
  - the industry specific risks relevant for the jurisdiction in which your company operates;
  - main principles of organisational governance in financial services organisation;
  - roles and assurance activities of the second line of defense functions within financial services that provide coverage of sector-specific risks; and
  - the relationship internal audit has with its external regulator and how to effectively manage expectations of the regulator while maintaining a reporting relationship to the board.

Reference:
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Foundations-of-Internal-Auditing-in-Financial-Services-Firms.aspx

HOW INTERNAL AUDIT CAN CULTIVATE A CULTURE OF INNOVATION

Many internal audit departments are struggling to keep up with fast-moving technologies and widespread change in the profession. Staying on track will require more than adopting new technology, it will involve adopting a new mindset. It's time for internal auditors to think differently.

That's not a new assertion; companies have been in a period of radical change for some time, and corporate leaders, internal audit experts, indeed internal auditors themselves, have implored the profession to change along with the companies they audit. But some caution that internal audit either isn't moving fast enough or is not making the type of wholesale overhaul it needs to stay relevant in a fast-moving, digital world.

It's true that innovation will come at a price, but it going to take more than money to truly migrate to an innovative mentality. Internal auditors will have to become comfortable with a constant state of change. They will have to learn how to remain flexible to move where the risks are at a moment's notice and abandon the business-as-usual outlook, where they conduct the same low-impact audits year after year.

Two Types of Innovation

The second type of innovation is adopting advancements in the internal audit department itself. Those technologies include advanced and predictive analytics, robotic process automation (RPA), continuous auditing, cloud-based GRC tools, and many others. These two types of innovation are related. The thinking is that internal audit organisations that seek to adopt a culture of innovation in their own processes will be more adept at keeping up with the innovations throughout their organisations, and therefore better equipped to audit them.

Slow to Move

What's holding internal audit back? One of the issues is time. Most internal audit departments are stretched thin and don't have the time to devote to coming up to speed on new technologies, even if it would save time in the long term. Another problem is that the technology is moving so fast that some CAEs decide they can't keep up with it all and throw up their hands.

Resources are also a problem. Gaining access to enabling technology skills and expertise remains a major challenge, and one that internal audit departments may also address through outsourcing and co-sourcing arrangements.

Promoting an Innovative Culture

Some advice on creating a culture of innovation, including:

Fix the underlying processes first: You can't innovate on top of bad processes or bad management. Those problems are hindrances to innovation and must be corrected first. Compare innovating bad processes to giving a bad driver a new car. It won't fix the problem and the driving will still be bad.

Set expectations and measure them: Dispelled the notion that innovation comes from big, bold moves and from sewing chaos, as we sometimes hear from Silicon Valley types. "Innovation, at least in an internal audit sense, is way more disciplined than that," he said. He advised attendees to set goals and stay on top of them. Achieve a measurable goal and then move the mark to the next one. "We may think that innovation is these huge breakthroughs, but it's not."

Focus on people: Another piece of advice to creating a culture of innovation is to trust the people that are in place, particularly those on the front lines. "To create innovation we have to give people the freedom to be honest, and we have to led them fail before they succeed,". Emphasised the need to be able to resolve conflict as part of the innovation process. "The inability to resolve conflict is fatal to the innovation process."

It's all about data: Three aspects that are driving innovation: the widespread availability of data, including unstructured data; the processing power that is now capable of analysing massive data sets much faster than in the past; and new software models, such as open source and cloud, that have created more collaboration and better algorithms. But data is at the center of it all.

What CAE should do?

Internal audit departments that fail to demonstrate innovation are less likely to convince boards and management to provide more resources, resulting in a death spiral of sorts that can be fatal to internal audit, or at least their CAE leaders.
As the pace of change accelerates, the need to create a culture of innovation will only become more critical.

Reference:
https://misti.co.uk/internal-audit-insights/how-internal-audit-can-cultivate-a-culture-of-innovation

INTERNAL AUDIT'S ROLE IN ASSURING WHISTLEBLOWING HOTLINES ARE EFFECTIVE

When it comes to preventing or detecting fraud, whistleblower hotlines remain among the best protection money can buy. They can also be an important tool for internal auditors to assess fraud risk and provide information that can increase the quality of audits and should be assessed on a regular basis.

An anonymous whistleblower hotline should be a critical piece of any organisation's anti-fraud efforts. Likewise, since the effectiveness of anti-fraud controls is a key area of concern for internal audit, auditors can and should be looking into company hotlines to ensure they are operating effectively and are prepared to handle tips that could possibly save their company thousands or even millions of dollars.

Benefits of a Hotline

Whistleblower hotlines allow organisations to leverage the power of the many—what we now call "crowd sourcing." By empowering everyone in the organisation (and everyone it interacts with) to report red flags or suspicious behavior, the eyes and ears of many individuals can provide a breadth of coverage to detect fraud that a dedicated team could never achieve.

There must be a person in senior leadership who ultimately owns and is accountable for the hotline, and it should be clear who that person is.

One of the few downsides to hotlines is that they tend to be passive, in that they typically do not seek out fraud, but instead wait for employees (and other parties) to provide tips. This means hotlines are not necessarily good at detecting fraud quickly, and since the longer a fraud goes on the more it generally costs, the most effective approach is to use a hotline in concert with other, more active fraud detection methods, such as audits, data analytics, and other monitoring tools.

Internal Audit Assurance of Whistleblower Hotline

Although hotlines are relatively inexpensive and easy to implement, that does not mean the company can take a "set it and forget it" approach to managing them. Indeed, there are many ways that internal audit can help provide assurance as to the quality and effectiveness of the hotline programme on an ongoing basis. Here are five areas to consider during audits of whistleblower hotlines:

1. Functionality and Organisation

The most basic thing internal audit can do is verify that the hotline exists and that it is in working order. Audits should include testing to ensure that phone numbers are operational, calls are routed properly, digital communications are transmitted properly.

In addition to basic functionality, internal audit can look into whether the hotline is adequately supported and has everything it needs in order to work effectively and accomplish its mission. This includes sufficient funding and access to resources, but it also includes staffing by qualified individuals with the training and expertise to handle the different types of cases the hotlines receives.

2. Communication

It is not enough, however, for the hotline to merely exist and be available to potential whistleblowers. In order for it to be effective, employees must be aware of the hotline, understand its purpose, and know how to use it. Therefore, internal audit should seek to understand the communications strategy for the hotline. Ideally, communication about the hotline will be incorporated into a broader communication effort around the company's ethics and anti-fraud efforts. This will help users to think of the hotline not just as a means for reporting bad behavior, but as a key part of the company's commitment to enforcing the code of conduct. It is also important that the hotline be regularly advertised in high-visibility areas.

There is no right number or quota of calls that the hotline should be receiving, but usage rates can provide clues as to the effectiveness of the hotline.

3. Compliance

Whistleblower hotlines by nature handle sensitive issues and information, and if these are not handled correctly, it is possible the hotline could expose the organisation to greater risk than it is designed to control. It is critical that management have a thorough and complete understanding of all external regulations and whistleblower laws, as well as internal company policies, with which the hotline must comply.

Internal audit should understand the hotline's compliance risk-assessment process and determine whether it is staying on top of changes (and variations, particularly for multinationals) in the regulatory environment. If the organisation contracts with a third party for hotline services, then internal audit should examine whether an effective third-party risk management process (including a right to audit clause) is in place around the hotline, particularly as it relates to data privacy and cybersecurity.

4. Performance

One of the key performance measures internal audit can use when looking at whistleblower hotlines is usage rates, or the number of calls and cases the hotline fields. There is no right number or quota of calls that the hotline should be receiving, but usage rates can provide clues as to the effectiveness of the hotline. For example, if there is a significant change in the historical trend of usage, internal audit should work with hotline management to understand the cause. Or, if the hotline is very seldom used, it could be an indicator that there is a lack of awareness of the hotline itself, or it may suggest that employees and other parties need additional education about red flags and the types activity they should report. Another possibility, which is a key risk related to hotlines, is that potential users do not feel comfortable or confident in using the hotline.

5. Case Files

Reviewing a sample of past cases gives internal audit the opportunity to address a number of important questions around the performance and effectiveness of a hotline. When reviewing past cases, auditors should explore questions such as:

- Is there a policy in place to guide the hotline staff's response to tips, and is that policy being followed?
- Are the people involved (hotline staff, subject-matter experts, senior leadership, etc.) doing a good job of following through from when tips are reported until they are resolved?
- Are tipsters' identities being kept anonymous where appropriate?
- Are tipsters being protected from retaliation?
- Are documentation and record keeping protocols being followed?

What CAE should do?

Determining the success of whistleblower hotlines is not always a straightforward endeavor. Nevertheless, there are indicators to review and questions that internal audit can ask to help provide assurance that this critical element of the company's anti-fraud arsenal is functional and effective. It is well worth the time to investigate whether the hotline is effectively reducing fraud risk, if the hotline itself is exposing the company to any risks, and if there are any enhancements to the hotline process that internal audit could recommend.

Reference:

https://internalaudit360.com/internal-audits-role-in-assuring-whistleblower-hotlines-are-effective/

HOW INTERNAL AUDIT CAN BETTER CONVEY RISKS USING A HEAT MAP

One of the effective tools in conducting risk assessment is a "Heat Map". The risk heat maps are a common part of an ERM approach to risk management. The Committee of Sponsoring Organisations' (COSO) ERM guide, *Enterprise Risk Management—Integrated Framework*, promotes the use of a risk matrix or heat map to focus management's attention on the most important threats and opportunities and to lay the groundwork for risk responses.

A heat map is a two-dimensional representation of data in which values are typically represented by colors (often red, green, and yellow) and can range in complexity from simple (for example, showing qualitative risks only) to more complex (including qualitative and quantitative risks).

In the risk assessment process, visualisation of risks using a heat map presents a concise, big-picture view of the full risk landscape to discuss while making decisions about the likelihood and impact of risks within the company.

Organisations use a variety of ways to identify entity-wide risks, including surveys, workshops, interviews with business unit managers, risk factors disclosed in financial reports, industry literature and many others.

Assigning the impact and likelihood scores is the most difficult part of the risk-mapping process and much thought and deliberation should go into it. While internal audit can play an important part in this risk scoring, the process should seek major input from the business unit managers, risk management function and elsewhere.

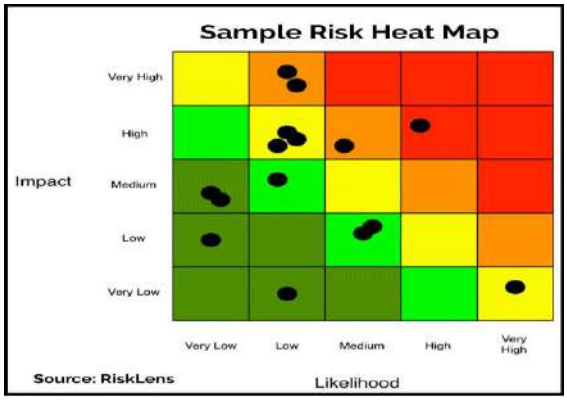
Plotting the Risk

A typical risk heat map will show risks plotted on a graph with "potential impact" on the vertical axis at left and the "likelihood" plotted on the horizontal axis along the bottom.

A simple 3×3 risk heat map will contain three categories for each. Potential impact can be defined as high, medium, and low, while likelihood can be defined as remote, possible, and plausible. Once each risk is scored on these attributes, they can be plotted on the graph.

A more complex map can have more categories, such as a 5×5 map. For example, potential impact can range from negligible, low, medium, high, and extreme, and likelihood can range from remote, unlikely, possible, plausible, to likely.

Again, it's more important that these terms are used commonly throughout the organisation than the exact terms used.



The map can help the company visualise how risks in one part of the organisation can affect operations of another business unit within the organisation. A risk map also adds precision to an organisation's risk assessment strategy and identifies gaps in an organisation's risk management processes.

Additionally, it helps to clarify the company's relative response to risks. Since there are limited resources to manage risks, the response must be in proportion to the risk. A heat map can help identify where resources are being used disproportionately to the threat implied in a given risk.

Eight Steps to Creating a Risk Heat Map

1. Define the Scope

Decide on the scope of the map you want to create. It can be a simple 3×3 matrix with three colors for high, medium, and low, or it can be a complex affair with layers based on types of risk, several categories on each axis, multiple shades depending on risk scores, lines that follow how risks have changed over time and more.

Start simple and add complexity as you go along. Also, ensure that those who will use the map in the decision-making process are on board with the planned scope.

2. Create a Common Language

Terms like "likelihood," "impact," and "onset speed" need to be defined and used in the same way throughout the organisation. It's also a good idea to give rankings along the axes quantitative ranks, such as percentage ranges or scale ratings, such as 1 out of 5 for "low." To create a common understanding of the organisation's risk profile.

3. Gather the Necessary Data

You may be consolidating data from several departments or functions, in which case you need to ensure that the assessments were done in the same way and that duplication is eliminated.

It is important to get a consensus on the data before you begin the mapping process. You don't want process owners taking issue with the risk scores after the map has already been created.

4. Score the Risks

Score on likelihood, impact and other factors you want on the map, according to the agreed scope. This part is likely done already, if a risk register or risk matrix is created after the risk assessment and identification process is completed.

It is important that process owners and those that "own the risk" drive the risk scoring process, since they are closest to it, with help from the second and third lines of defense.

5. Plot the Points and Create the Map

The actual mapping of risks is fairly easy, once the data is gathered and consensus is achieved on scores. Use a simple application, such as Excel, at first and for simple maps. In fact, Excel should serve most of your heat-mapping needs.

More sophisticated programmes, such as Tableau or eSpatial, may be able to do slightly more. Large ERM software packages will also likely be able to produce risk heat maps from existing risk-assessment work, without re-entering lots of data.

6. Assess the Relative Placement of Individual Risks

At this step, such problems can be identified. You should assess the usefulness of the map at this stage. Is there too much data incorporated into the map to make it useful? Is it too complex? Too cluttered? Too simplistic?

You won't really know until you plot the points and put it all together. At this stage, the complexity or scope can be adjusted to ensure the usefulness of the final product.

7. Gather Feedback

The feedback and consensus process starts again with the whole map in view and adjustments are made to fix outliers, errors, and in light of the relevant scores of each risk. The usefulness, based on complexity and addressed in the last step, can also be further assessed and adjusted here. It might also be time to incorporate feedback from senior executives or even the board.

8. Refine and Update the Map

Use the feedback to make adjustments to the map and then create the process for updating the map and ensuring that it is a living document. It is an annual process to coincide with the risk assessment that is completed as part of the audit planning stage? Or will it be updated on a quarterly, monthly, or more frequent basis? At each iteration, the map can also be refined and more complexity can be added as those in the organisation become more familiar and comfortable with using it.

Seven (7) Ways for Improving Risk Heat Maps

1. Separate the "impact ratings" for different kinds of risk (for example, financial, operational, and strategic risks).

2. Add layers to traditional impact and likelihood displays. Display additional variables like risk velocity and control effectiveness.

3. Demonstrate the effectiveness of risk mitigation plans by including inherent and residual risks. Illustrate reductions in risk exposure based on mitigation and internal controls.

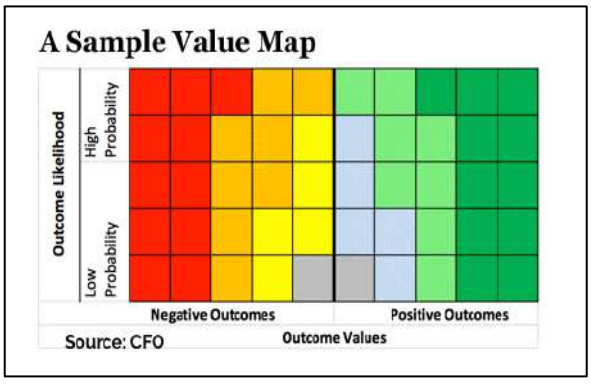
4. Differentiate zones of acceptable and unacceptable risk exposure on the heat map.

5. The display changes over time by demonstrating movements in risk exposure value.

6. Establish risk reduction targets by inserting desired risk levels that can instigate conversations about specific mitigation activities.

7. Filter the risk assessment data to show different perspectives across the organisation.

A Sample of Value Map



You may also include quadrants for favorable outcomes too. The value map has a side for opportunities in addition to the threats.

Limitation with Using a Risk Heat Map

It provides a fairly simplified view of the overall risk picture, rather than a comprehensive cataloging of risk, that can be found in the risk register.

1. It is a Point-In-Time Report

When management and the board rely on the review of a report that purports to show the top risks to the organisation and their condition, they may end up reviewing the information that is out of date, unless they are reviewing a dynamically changing report.

2. It is Not a Complete Picture

It can never be a comprehensive view of all risks, especially since risks change at every decision and at large companies the full risk landscape likely includes risks too numerous to plot on a two-dimensional page. And, it doesn't portray the risks that haven't been or can't be identified.

3. It Doesn't Always Identify the Risks that Need Attention

Just because a risk rates 'high' because the likelihood of a significant impact is assessed as high doesn't mean that action is required by senior management, or that significant attention should be paid by the board. They may just be risks that are 'inherent' in the organisation and its business model, or risks that the organisation has chosen to take to satisfy its objectives and to create value for its stakeholders and shareholders.

4. It Only Shows Impact and Likelihood

Risk heat maps can capture more complexity, such as the change over time and residual vs. target risk profile, but for the most part, most risk heat maps show impact and likelihood. Adding too much more and they start to lose the "at a glance" picture they are intended to give.

5. The Assessment of Impact and Likelihood May Not be Reliable

The risk heat maps don't immediately show the source of the information and data, including how the likelihood and impact scores were determined and they could be possibly wrong.

6. It Doesn't Show Whether Objectives are in Jeopardy

It is very important to produce and review a report that highlights when the total effect of a risk source, considering all affected objectives, is beyond acceptable levels. While it may not significantly affect a single objective, the aggregated effect on the organisation may merit the attention of the executive leadership and the board.

Regardless of the abovementioned limitation, the intention of the risk heat map is to provide more of an "at a glance" view of risk in the organisation than to be the guiding tool for managing risk.

What CAE should do?

CAE should understand that no risk heat map is perfect, and it certainly shouldn't be the only or even main tool for making decisions around risk. Nevertheless, CAE may use a risk heat map as a tool to communicate the overall risk picture to C-Suite level.

Reference:

https://misti.com/internal-audit-insights/how-internal-audit-can-better-convey-risks-using-a-heatmap

APPLYING AGILE PRINCIPLES TO INTERNAL AUDIT

Many internal audit shops are adopting Agile project management principles in an attempt to create a more flexible, adaptive and customer-oriented audit function.

Agile increases team productivity and employee satisfaction. It minimises the waste inherent in redundant meetings and repetitive planning.

The following tools such as MoSCoW, Sprints, Kanban and Shu Ha Ri for Agile audit execution invaluable for continually improving the ability to deliver audit services, while improving communication and collaboration.

MoSCoW

We use the MoSCoW technique to prioritise and plan internal audit activities. The MoSCoW method is an acronym, which stands for: "**Must Have**, **Should Have**, **Could Have**, and **Will not Have**." (The "o's" have been added only to spell out the familiar city to make the term easier to remember.) This method allows internal audit to reach a common understanding with stakeholders on the importance they place on the delivery of audit activities that could generate the most value.

MoSCow also reminds auditors to develop a laser focus on what's most important from an audit coverage standpoint in a constrained environment. This is especially important given that more and more auditors are being asked to do more with less. Using MoSCoW can enable internal audit teams to more efficiently manage scope, focus on key issues and drive better allocation of resources.

However, it is difficult to embrace prioritisation methods such as MoSCow when auditors are used to the habit of covering everything on a specific audit. Embedding MoSCoW and deriving value from it requires time, experience and open minds.

Sprints

This enables the internal audit team to remain focused and committed to completing the required tasks within the allotted time. A shift in auditor mindset, where during a sprint the entire internal audit team demonstrates urgency and determination to resolve any roadblocks and drive towards the finish line.

A sprint typically has four (4) components to manage the workflow of the given project:

1) Sprint Planning Meeting
A focused meeting to cover all the expectations of the sprint, who is responsible for what, and how it will be accomplished.

2) Daily Stand-Ups
Daily timed briefings on what was accomplished the prior day, the goals for the next 24 hours, and any hurdles that may be in the way of meeting those goals.

3) Sprint Review
A meeting between internal audit and stakeholders to review the work, obtain feedback and discuss the results of the sprint.

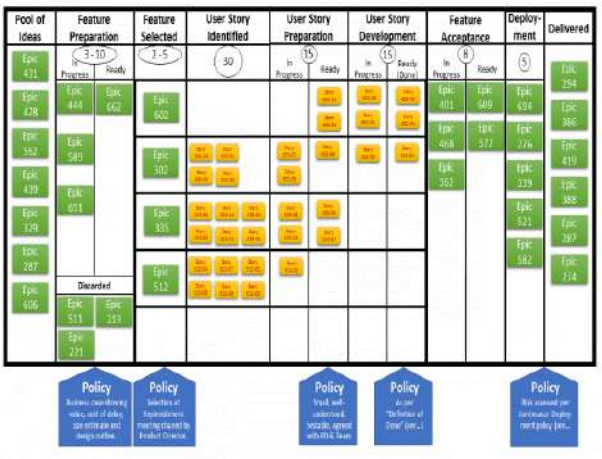
4) Sprint Retrospective
A meeting to discuss how the sprint went and how the process can be improved for the next sprint.

Kanban

Kanban is a simple yet visually effective tool to monitor progress on internal audit activities and can help propel an Agile internal audit initiative. It contains specific activities that need to be performed, activities in progress, and activities that have already been completed.

Whilst application of Kanban boards vary from organisation to organisation and can be digital or physical.

Kanban boards enable an end-to-end, real-time view of a project's status, helping teams focus, prioritise activities and highlight delays. It is a great project management tool to facilitate candid dialogue with stakeholders during the Sprint Review event and foster collaboration across the cross-functional internal audit team during events such as Sprint Planning and the Daily Stand-Up.



Shu Ha Ri

Introducing an Agile approach to auditing means transformative change and requires a shift in the mindset of internal auditors. The Shu Ha Ri, the Japanese philosophy can provide structure and aid in change-management processes.

Shu Ha Ri is a concept to describe different levels of training or learning, and while it was developed in a martial art setting, it can be applied to Agile to help us along our journey to implementation.

Shu Ha Ri involves three types of learning or training styles.

2) "**Shu**" Stage
The student follows the form and disciplines of the master closely, repeating the basics and structures without deviation, with the goal of mastering the techniques. Once mastered, the student can begin to depart from the forms, moving into the "Ha" stage.

By initially focusing on the "Shu" principle, internal auditors are encouraged to learn the fundamentals and get comfortable with the basics. In a highly regulated industry, such as financial services, Shu also facilitates the transition with minimal to no change in auditing methodology.

3) "**Ha**" Stage
The student is experimenting with new ways and applications of what was already mastered and innovating on them. The student learns more about the underlying principles and theory behind the techniques.

As internal auditors gain experience in delivering internal audit projects using the Agile approach and gain confidence, it is imperative that internal audit organisations continue to evolve and find ways to make the auditing process more Agile friendly.

This continuous improvement process is essentially the "Ha" stage, a stage where internal audit is not afraid to explore the limitations on the way things are done and push the boundaries of such limitations.

1) "**Ri**" Stage
The student learns from his practice, arriving at a new place and adapting what he or she has learned to new circumstances.

The "Ri" stage is about mastering Agile internal auditing to the point that this becomes the norm.

What Internal Auditors should do?

The journey of an agile transformation is not easy and requires multiyear planning, sponsorship from senior management, learning the ceremonies of Agile techniques, the patience to master those techniques, the education of stakeholders and the continued drive to build an ecosystem that continuously promotes an Agile mindset.

Internal auditors should consider adopting this Agile internal audit path where the internal audit is not only providing a better service for its clients, but where they can work happier and smarter.

Reference:
https://misti.co.uk/internal-audit-insights/applying-agile-principles-to-internal-audit

THE BUSINESS OF ETHICAL AI

Governments are questioning on the trustworthiness of artificial intelligence, but will businesses be as cautious?

According to Angel Gurría from Organisation for Economic Co-operation and Development (OECD) emphasised that for artificial intelligence (AI) to reach its potential, people must be able to trust it. He added the "Ethics is the starting point," that can divide what you should do and what you should not do with this kind of knowledge and information and technology.

Businesses Aren't Worried

Survey has been conducted and the result shows more than 5,300 employers and employees in six countries, nearly two-thirds of employers say their organisation would be using AI by 2022.

However, based on the survey:

- 54% of employers - aren't concerned that the organisation could use AI unethically.
- 52% - aren't worried that employees would misuse AI.
- one-fourth of these employers - are concerned about future liability for "unforeseen use of AI,".
- 23% of employers - have a written policy for using AI and robots ethically.
- Among employers that lack a policy, 40% - say their organisation should have one.

Chief Marketing officer at Genesys, Merijn te Booij, says that "We advise companies to develop and document their policies on AI sooner rather than later. Those organisations should include employees in the process. Also, he advises, "to quell any apprehension and promote an environment of trust and transparency".

Head of Data Science at SAS UK and Ireland, Iain Brown emphasised on "Trust is still foundational to business", and one-fourth of consumers will act if they think an organisation doesn't respect or protect their data. He advises asking three questions to determine whether the organisation is using AI ethically:

- Do you know what the AI is doing?
- Can you explain it to customers?
- Would customers respond happily when you tell them?

Governments Propose Guidelines

Building ethical, trustworthy AI is at the core of the several plans, guidelines, and research initiatives sponsored by governments and non-governmental organisations.

The European Commission guidelines set out seven requirements for trustworthy AI:

- AI should empower people and have appropriate oversight.
- AI systems should be resilient and secure.
- AI should protect privacy and data and be under adequate data governance.
- Data, system, and AI business models should be transparent.
- AI should avoid unfair bias.
- AI should be sustainable and environmentally friendly.
- Mechanisms should be in place — including auditability — to ensure responsibility and accountability over AI.

What Internal Auditors should do?

The varying strands of AI ethics development are in the early stages, though. Meanwhile, the technology is advancing well ahead of any standards. In his speech in London, OECD's Gurría said AI can benefit society if people have the tools and the tools can be trusted. He added "Artificial intelligence can help us if we apply it well,".

Reference:
https://iaonline.theiia.org/2019/Pages/The-Business-of-Ethical-AI.aspx

TRANSFORMING ASSURANCE

Data analytics and automation can enable IA to provide enhanced assurance for organisational risks.

The IIA's Core Principles for the Professional Practice of Internal Auditing *use the term* risk-based assurance instead of reasonable assurance, which implies that there are different levels of assurance based on multiple risk factors. That creates an opportunity for IA to move its work to a higher level by delivering enhanced assurance to the board and management.

Enhanced assurance does not imply reductions in risk. Instead, it refers to asking better questions about the risks that matter as well as the risks that should be automated for greater efficiency. It's about developing assurance at scale to cover the breadth of operations and strategic initiatives efficiently and cost-effectively.

Today's technologies can enable internal audit functions to automate their operations and provide enhanced assurance by referring to the strategy as follows:

Better Teams

- *Small, focused teams* are more productive than large, consensus-driven teams directed from the top down, author Jacob Morgan notes. By having more people on the team increases the communication needed and bureaucracy, which can slow the team down.
- *Collaboration with automation* - modernise the performance of small teams.
- *Intelligent automation* - integrate oversight into operations, reduce human error, improve internal controls, and create situational awareness where risks need to be managed.
- *Automation* - enabled collaboration can help reduce redundancies in demands on IT departments, as well.

The Human Element

- The biggest assurance risks are related to people, but too often the weakest link is related to auditing human behavior.
- Hence, the vulnerabilities in human behavior and the intersection of technology represent a growing body of risks to be addressed.
- Based on studies from IBM - human error is a key contributor to operational risk across industry type and represents friction in organisational performance.
- The benefit of automation can create an opportunity to reduce human error and to improve insights into operational performance.
- Hence, CAEs can collaborate with the compliance, finance, operations, and risk management functions to develop automation that supports each of these key assurance providers and stakeholders.

The Role of Technology

- To enhanced assurance by leveraging analytics to ask and answer complex questions about risk.
- To improve situational awareness in audit assurance.
- *Intelligent automation* addresses issues with audit efficiency and quality.
- *smart automation* - leads to business intelligence. As more key processes are automated, they provide insights into changing conditions that may have been overlooked using periodic sampling techniques at points in time.

Steps to Enhanced Assurance

Before buying automation, CAEs should answer three questions:

1. How will automation improve audit assurance?
2. How will automation make processes more efficient?
3. How will auditors use it to improve audit judgment?

The CAE should consider automation –as an opportunity to raise awareness with the board and senior executives about enhanced assurance and better risk governance. To do so, internal audit must align enhanced assurance with the strategic objectives of senior executives.

To implement enhanced assurance in the internal audit function, CAEs should follow three steps:

- Identify the greatest opportunities to automate routine audit processes.
- Prioritise automation projects during each budget cycle in coordination with the operations, risk management, IT, and compliance functions.
- Consider the questions most important to senior executives. i.e. How well do we understand risk uncertainties across the organisation? Do existing controls address the risks that really matter?

Assurance and Transformation

Forward-looking internal audit departments already are delivering enhanced assurance by strategically focusing on the roles people, technology, and automation play in creating higher confidence in assurance. Other audit functions are in the early stage of transformation.

What Internal Auditors should do?

- Automation works best at solving high frequency events that are routine and add little value in terms of new information on known risks. Instead of focusing on the shape of risk, auditors will be able to drill down into the data to understand specific causes of risk.
- Although these audit functions will make mistakes along the way, now is the time for them to build new data analysis and data mining skills, and to learn the strengths and weaknesses of automation. As these tools become more powerful and easy to use, enhanced assurance will set a new high bar in risk governance.

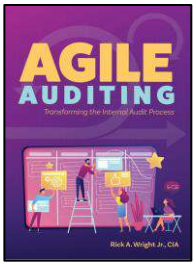
Reference:

https://iaonline.theiia.org/2019/Pages/Transforming-Assurance.aspx

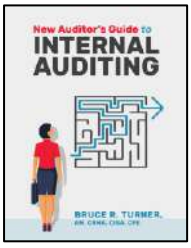
BOOK'S REVIEW

NEW RELEASES! **ORDER NOW!!**

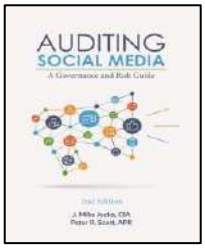
1) Agile Auditing: Transforming the Internal Audit Process



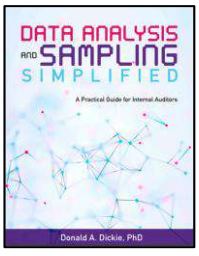
2) New Auditor's Guide to Internal Auditing



3) Auditing Social Media: A Governance and Risk Guide, 2nd Edition



4) Data Analysis and Sampling Simplified: A Practical Guide for Internal Auditors



Reference:

https://www.iiam.com.my/wp-content/uploads/2017/08/Book-Order-Form.pdf