IIA Malaysia e-techline
August 2022 Issue 4/22

STANDARDS AND GUIDANCE

BUILDING AN EFFECTIVE INTERNAL AUDIT ACTIVITY IN THE PUBLIC SECTOR (BY IIA GLOBAL)

The public sector chief audit executive (CAE) is charged with preparing the internal audit activity to respond to increasing challenges and demands for transparency, accountability, and effectiveness at all levels of government and other public sector enterprises. Accomplishing this task may involve establishing a new activity or improving or rejuvenating an existing one that is performing at a less than optimal level. Adding to the demands, the CAE also may be new in the position. As part of their response, the CAE needs to understand the unique aspects of the public sector environment, including threats — political and otherwise — to the internal audit activity's independence.

Internal and external stakeholders, especially the public the organisation serves, rely on the assurances provided by the internal audit activity to ensure that efficient, effective, and equitable use is being made of public funds and the organisation is operating in the public interest.

This guidance touches on all seven of the Public Sector Context criteria, or unique aspects of working in the public sector environment, which include:

- **Accountability in Public Funding**
  Internal audit must consider effective use of public funds as part of the audit plan and should consider controls in all organisational processes to protect the reliability and integrity of financial information.

- **Nature of Politics**
  As part of evaluating culture risk, and to align with the IPPF's Code of Ethics, the public sector internal audit activity must develop an understanding of political interests.
  The results of internal audit work should be disseminated appropriately, even outside the organisation, to improve governance, risk, and control processes, but not for political purposes.

- **Governance**
  Internal audit is an integral component of effective governance and helps organisations achieve their objectives and measure their results. If the organisation does not have strong and mature governance processes in place, it may not be adequately prepared for an effective internal audit activity. Internal audit must reflect on and be aligned with the governance of the organisation.

- **Public Good/Public Interest**
  Although typically the internal audit activity does not report directly to the public, all public sector internal audit work should be done on behalf of the public and with the public benefit and interest in mind. The internal audit activity must be assessing what the organisation is doing to provide value to the public.

- **Transparency, Ethics, and Integrity**
  Public sector internal auditors must display the highest level of ethics and integrity in their work with the organisation to establish and maintain credibility with internal audit stakeholders, both inside and outside the organisation.

- **Legal, Regulatory, and Fiscal Compliance**
  The internal audit activity must become familiar with the laws, rules, and regulations that govern the organisation and consider legal aspects while conducting all assurance and consulting work. Additionally, the internal audit activity must ensure the appropriate governance structure has been established for the activity to ensure it is in compliance with any laws, rules, and regulations affecting internal audit operations within the organisation.

... 1

- **Efficiency, Effectiveness, and Equity in Public Service Delivery**

  The ultimate customer of all public sector services is the public. Therefore, public sector internal auditors must consider this important element in planning all assurance and consulting engagements to ensure the results of assurance and consulting work add value to the organisation and ultimately the public. This includes audits focused on government performance and achievement of outcomes.

Developing the Internal Audit Activity

- **Ethics and Professionalism**

  Ensuring the utmost ethical conduct and actions of integrity at all times helps provide the credibility needed by the internal auditor to effectively communicate recommendations for improvement to management and public sector audit committees (governing bodies).

- **Establishing Governance for the Internal Audit Activity**

Inputs - Standards and Requirements	- IIA Standards - Government Auditing Standards - Specialty Standards - Public Sector Requirements
Activity - Delivery Models	- Insourcing - Outsourcing - Cosourcing (or partnering)
Activity - Stakeholder Identification	Identify Internal Audit Stakeholders

Internal	External
Board or governing body	Governing body
Head of the organization	Elected officials, including legislative committee members
Audit committee	Regulatory bodies
Executive, senior managers	Private citizens
Human resources	Third-party service providers
Legal counsel*	External auditors
Audit clients	Other assurance providers
Internal service providers	Counterparts in similar organizations
Staff auditors	Professional associations such as The IIA
Staff suditors	Local professional leaders
	Media

* May be internal or external depending on organization's size, structure, and other factors.

Activity - Establishing Reporting Relationships	- Establishing Reporting Relationships
Output - The Charter and Audit Committee	- The Internal Audit Charter - Creation and Operation of the Audit Committee
Additional Considerations	- Collaboration with Other Audit Activities - The Internal Audit Capability Model (IA-CM) for the Public Sector - Utilizing the Three Lines Model - Considerations of Governance, Risk Management, and Control - Consideration of Fraud - Environmental, Social and Governance (ESG) Considerations

... 2

Additional Considerations	- IT Considerations - Financial Management and Internal Control

Developing the Internal Audit Activity

- **Strategic Plan**

  A strategic plan helps the internal audit activity establish high-level goals for achievement in alignment with the organisational goals (and in the public sector, potentially the overarching government's goals as well).

  The CAE may begin strategic planning by taking stock of key organisational matters and their understanding of the organisation's culture, risks, and operating environment. It is important to understand the organisation's goals and how they relate to the goals of the internal audit activity.

- **Staffing the Internal Audit Activity**

  The internal audit activity should include personnel from diverse backgrounds and different levels of experience. In the public sector, the size of the internal audit activity most likely will be established through the budget process.

- **Creating a Budget for the Internal Audit Activity**

  Whether the CAE will be responsible for developing a budget may depend on where the internal audit activity resides within the organisation, as well as the size of the activity and the public financial management rules that apply to each government jurisdiction.

- **Establishing an Internal Audit Policies and Procedures Manual**

  Standard 2040 - Policies and Procedures states "The chief audit executive must establish policies and procedures to guide the internal audit activity.".

- **Quality Assurance and Improvement Program**

  According to *Standard* 1300 - Quality Assurance and Improvement Program, "The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.".

Performing Internal Audit Services

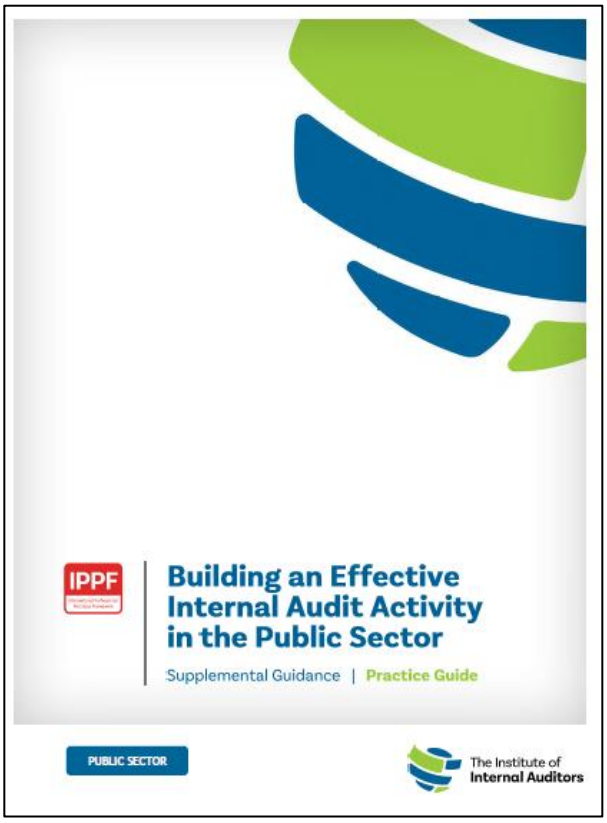
Inputs - Planning	- Define the Audit Universe - Perform an Entity wide Risk Assessment - Develop a Risk-based Audit Plan
Activity - Performing Engagements	- Planning Individual Engagements - Conducting Engagements - Gathering Sufficient, Reliable, Relevant, and Useful Information - Audit Engagement Supervision
Output - Reporting and Monitoring	- Communicating Results - Follow-up and Monitoring - Assessing Feedback

What should Internal Auditors do?

IPPF *Standard* 2120 – The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

IPPF *Standard* 2130 – The internal audit activity must assist the organisation in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

Internal audit must consider effective use of public funds as part of the audit plan and should consider controls in all organisational processes to protect the reliability and integrity of financial information.



Reference:
https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/building-an-internal-audit-activity-in-the-public-sector/

STANDARDS AND GUIDANCE

AUDITING CAPITAL ADEQUACY AND STRESS TESTING FOR BANKS 2ND EDITION (BY IIA GLOBAL)

For the economy to remain stable, banking institutions,' especially those that are systematically important (or "too big to fail") must have sufficient capital to handle changes in business cycles. This guide explores internal audit's role in evaluating the capital planning and management process.

- **Business Significance: Risks and Opportunities**

  Capital adequacy preserves the short- and long-term stability of financial corporations in managing the following risk exposures:

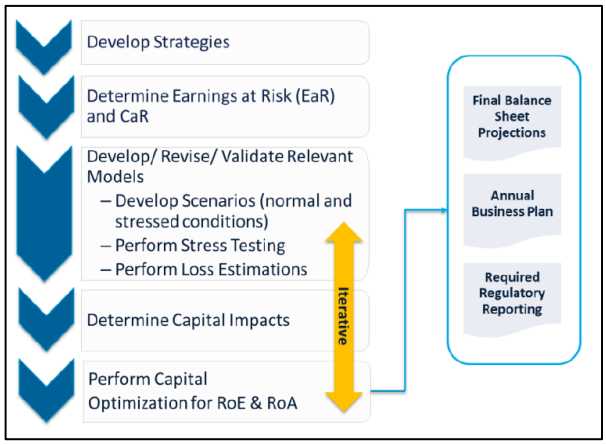
Credit Risk	The potential that a bank borrower, or counterparty will fail to meet its obligations in accordance with agreed terms.
Liquidity risk	The risk that the firm will not be able to meet efficiently both expected and unexpected current and future cash flow and collateral needs without affecting either daily operations or the financial condition of the firm.
Market risk	The risk of losses in on- and off-balance sheet positions arising from movements in market prices.
Operational risk	Risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.

These risk exposures may lead to outcomes including:

- Inability to expand the business.
- Inability to carry additional risk with available capital.
- Inability to distribute profits, such as dividends.
- Inability to meet financial obligations when they come due.
- A need to cease operations or receive assistance (such as bailouts) from the government.

The Capital Planning Process

Capital planning is key to the safety and soundness of a financial institution, and an institution's board is ultimately responsible for strategic decisions, including capital adequacy.



Overview of Regulatory Capital

- **Tier 1 Capital**

  Tier 1 capital is known as going concern capital, which means it enables the bank to absorb losses without needing to cease trading activities. In other words, the bank remains viable and operational even when it has suffered significant losses.

- **Tier 2 Capital**

  Tier 2 capital (CET2) is also known as gone concern capital, which means the business is no longer viable. This type of capital represents the less liquid, lower-quality assets to be consumed in a fatal situation for the bank.

- **Supplementary Capital: Capital Conservation Buffers, Countercyclical Buffers**

Capital conservation buffer	designed to ensure that banks build up capital buffers outside periods of stress that can be drawn down during periods of stress.
Capital countercyclical buffer	designed to achieve the macro-prudential goal of protecting the banking sector from periods of excessive credit growth, which is often associated with the buildup of system-wide risk.

- **Capital for Market Risk**
  - Standardised approach
  - Internal Models Approach

- **Operational Risk**
  - Advanced Measurement Approach
  - Standardised approach

Planning Engagements to Assess Capital Adequacy

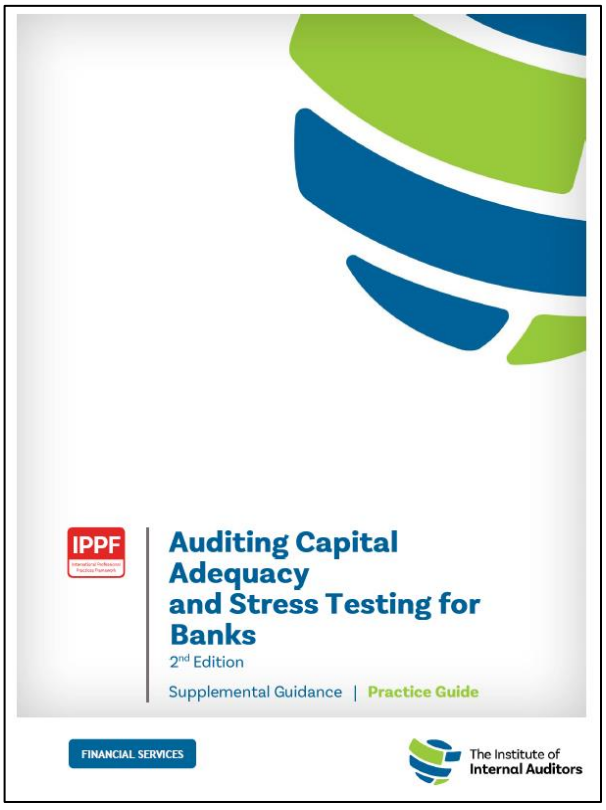
1. Gathering Information.
2. Conducting the Preliminary Risk Assessment.
3. Establishing the Engagement Scope.
4. Allocating Resources.
5. Performing the Engagement.
6. Communicating the Results of the Engagement.

What should Internal Auditors do?

IPPF *Standard* 1210 - Proficiency specifically identifies internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Internal auditors in the financial services sector must be qualified to understand, measure, and assess whether an institution's capital planning process adequately and effectively predicts the level of capital needed under current conditions, as well as under stressed financial and economic scenarios.

Internal auditors should understand the relationship among strategy, risk appetite, and the capital planning process and should be able to evaluate whether the three elements are an integrated unit or whether impediments interfere with managing capital risk in an integrated fashion. Concerns should be reported to the board.



Reference:
https://www.theiia.org/en/content/guidance/recommended/supplemental/practice-guides/auditing-capital-adequacy-and-stress-testing-for-banks-2nd-edition/

INTERNAL AUDIT FOUNDATION

INTERNAL CONTROL AND THE TRANSFORMATION OF ENTITIES (BY INTERNAL AUDIT FOUNDATION, ASSOCIATION OF CHARTERED CERTIFIED ACCOUNTANTS (ACCA), AND INSTITUTE OF MANAGEMENT ACCOUNTANTS (IMA))

Internal control is one of the fundamental concepts used by entities to achieve important objectives, improve performance and build reputation, especially in disruptive and uncertain times. Internal control forms a core part of the activities of accountancy, finance, and internal audit professionals, assisting them in ensuring that entities operate effectively. Yet the nature of the business model is changing for many.

Transformation, including the adoption of digital enablers, is changing the way that processes are undertaken. Rapid response to changing customer and economic factors is a reality. The report explores these and other emerging trends, their impact on internal control and the need for internal controls to be agile and future-ready to support business transformation and growth.

Effective internal control is one of the essential enablers for entities to grow with confidence and integrity in a multi-stakeholder world filled with volatility, uncertainty, disruption, and complexity. Internal control goes beyond statutory compliance requirements; it helps entities build trust, confidence, and a positive reputation in achieving strategic business outcomes. Effective internal control requires an appropriate combination of people, processes, technology, and data underpinned by an unwavering commitment to trust and ethics.

Current Challenges and Opportunities

- **Impact of Transformation**

  These reports stress the continuous nature of transformation for entities and the need to ensure that they can benefit from agile approaches to rapidly address current challenges. The continuous cycle of transformation embraces the application of technology and data-driven approaches, accepting that neither can be the primary driver for transformation itself.

  Drivers of change potentially disrupting internal control are below:

  - Geopolitical
  - Supply chain
  - Regulation
  - Consumer patterns
  - Climate
  - Economic pressures
  - Data
  - Technology

- **Technology Adoption**

  The reality of transformation is that it is not a department-level activity, it is an entity-wide one which has varying impacts in different areas. With inflationary pressures also growing, the drivers for automation increase and the ability of transformation initiatives to enable this is becoming increasingly important.

- **Data Flows, Big Data and Continuous Monitoring**

  Explosion of data is one aspect of the transformation journey for many entities as they seek to use data in ways that enable them to understand their customers better, among other activities, and streamline their processes.

  One of the challenges with such volumes of data is that traditional sampling techniques become challenged in ensuring that appropriate conclusions are drawn from testing – several roundtable participants referred to this. The opportunity to use computing power to constantly review the totality of a population, so called 'continuous monitoring', may offer advantages in internal control monitoring.

- **Evolving Ways of Working**

  Transformational changes are not related only to technology and data. Rather, they are often fundamental shifts in the ways of working. One lesson from the pandemic is that those entities that have managed the challenges more effectively are those that have adopted collaborative and innovative cultures.

  Working from home has heightened the risk profile for many entities around the loss of intellectual property.

- **Non-Financial Reporting**

  It is very important that for investors and other stakeholders that there be trust and confidence in ESG/sustainability disclosures such as those on climate risk, carbon emissions, cybersecurity, innovation, and human capital.

  This data, reporting and analysis is different from financial data in that it tends to be more unstructured, qualitative, and estimated from different sources. Data governance, quality, modelling, and analytics are critically important.

Evolving Our Thinking

- **Charting A Way Forward**

  Understanding the risk profile is essential. Controls monitor risks and this link in the transformed entity remains essential. The automation of controls, including the use of machine learning and other techniques, requires this to be in place.

  This, in turn, should integrate with the governance risk and compliance (GRC) platform that forms part of the overall technological architecture.

Technology and Data Evolution

There is no escaping that technology and data are changing the business landscape.

The impact of the 'fourth industrial revolution' on entities is increasing, especially as they seek to address the economic climate that is emerging in 2022. An increased use of automation in the production cycle will affect not only manufacturing-based entities but those across all sectors in all areas of operations.

The Agile Entity

The economic drivers of 2022 and beyond are likely to mean that entities will need to be agile in adapting their operating models. Agility means that there is a need to constantly update and change the operating model to be able to exploit the opportunities and manage the constraints of the economic environment. This means that internal controls need to be adaptive and dynamic.

As entities increasingly migrate to Cloud-based technology and data architectures built around 'best of breed' applications, the need to exploit this agility will increase.

It is important that those charged with internal control across all levels of operation within the Three Lines Model ensure that these considerations are included in the project teams that are responsible for driving these agile changes. As the breadth of internal control increases to include more non-financial as well as financial aspects of the entity, so there is a need for an integrated view of risk data.

Non-Financial Reporting Considerations

The reporting profile of entities is changing. Stakeholders are requiring a broader view of performance that includes ESG considerations; indeed, the range of these stakeholders themselves is increasing.

Details of The Implications for Internal Control

- Around or through.
- Changing working environment.
- End-user developments and the use of Lo-code / No-code solutions.
- IT general controls.
- Blockchain.
- Machine learning and artificial intelligence.

Skill Sets

There is a clear need to develop a broad range of skills both technical and more inter-personal in nature. As internal control continues to transform, so the skill sets of those charged with it need to expand. An appreciation of technology and data are no longer 'nice to have', rather, they are necessities.

The importance of Big Data and the transformation process requires that each line of the Three Line Model needs to ensure that staff have the appropriate skill sets to manage the risks. At a time when, for many entities, resources are constrained for several reasons, this presents a significant challenge, but one that cannot be ignored.

Real-Time Data Considerations

The potential of using data inspection techniques such as embedded code to identify potential patterns in transactions in real time offers an opportunity not only to make the performance of a control more proactive but also to increase the value added to entities.

It is important to strike a balance between the continuous monitoring of data and the identification of transactions that might require further investigation, with the assessment of strategic risks and subsequent audit work.

The efficient automation of controls depends upon several factors:

... 8

- an understanding of the capabilities of the application to validate transactions as part of the workflow.
- building into that workflow the appropriate levels of oversight.
- using reports to monitor the performance of the process, identify trends and isolate outliers for investigation.
- using the workflow intelligently to document the control activities.
- using bespoke developments and end-user tools, such as RPA, to develop monitoring controls.

Data Governance – A Question of Internal Control?

If internal control is to broaden in its scope to embrace data that is used for both financial and non-financial performance and reporting objectives, then the integrity of that data becomes ever more important. Nonetheless, from a different perspective, this is also the objective of those charged with data governance.

A Question of Strategy and Culture

An internal control framework exists to 'to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance' (COSO 2013). Implicit in this is the link to the management of risk. That can only be achieved by a strong culture of risk management and a reinforcement of the purpose of internal control. This culture must be established by the entity's senior leaders.

Implications for Internal Control Frameworks

There is an appreciation of the need to embrace digitalisation and transformation, but a lack of understanding of how to do this was cited as a barrier. Any guidance will, inevitably, be generic and while it can provide an element of support it cannot provide the specific context in which an accountancy and finance professional, wherever operating at which ever line will need to apply it.

What should Internal Auditors do?

IPPF *Standard* 1210 - Proficiency specifically identifies internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

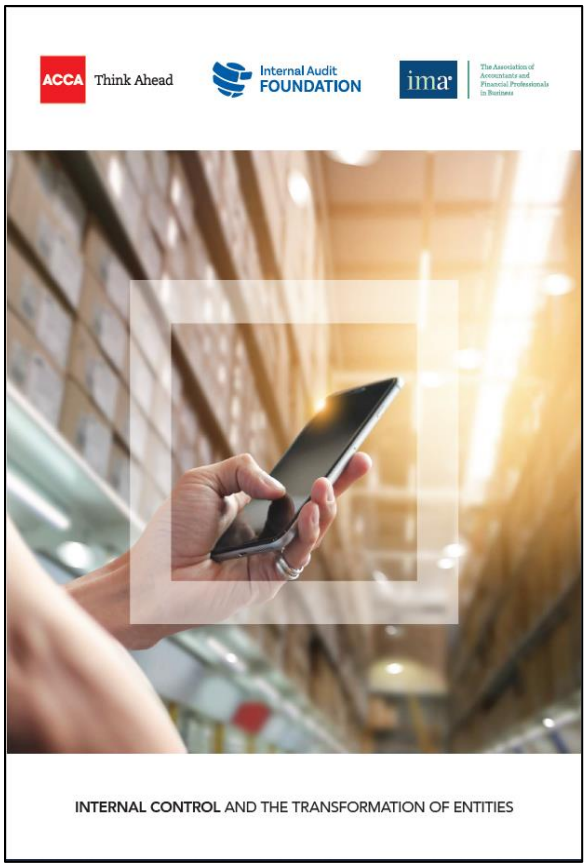
The availability of the right skills is fundamental to the maintenance of effective internal controls. These skills are broadening beyond the purely financial and there must be recognition of this expanded need and the consequent investment required both by entities and individuals.

In a fast changing and expanding business environment (including drivers such as technological developments and ESG), effective internal control helps to build confidence, trust, and reputation.

For internal audit professionals, it is important to have a detailed appreciation of the opportunities that technology can present and how these are translated into processes enacted and the optimised ways of working.

IPPF *Standard* 1230 – Continuing Professional Development specifically identifies internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

Through professional qualifications and continuous learning, these professionals need to ensure that they can maintain relevance, enabling them to guide decision makers in addressing the broadening governance and control requirements. In this way internal audit professionals are ready and able to guide their entities and the stakeholders into a new era for internal control.



Reference:
https://www.theiia.org/en/internal-audit foundation/latest-research-and-products/

INTERNAL AUDIT FOUNDATION

EMBEDDING ESG AND SUSTAINABILITY CONSIDERATIONS INTO THE THREE LINES MODEL (BY IIA GLOBAL AND WBCSD)

Sustainability presupposes an inside-out lens as it describes how organisations impact society and the environment. Sustainability initiatives can include a company's efforts to reduce its impact while creating value on the external environment (e.g., responsible sourcing or regenerative agriculture).

Environmental, social and governance (ESG) considerations presuppose an outside-in focus on how ESG issues (e.g., climate change) impact the company and its value by posing new risks, threats, and opportunities. ESG considerations are data driven and inform stakeholders on the value of a company by quantifying the impact of ESG issues on financial performance.

- **Corporate Culture and Behavior Change**
  Corporate purpose and culture are equally important, as they show leadership while characterising the extent to which the leadership values and remunerates ESG performance within the operations of an organisation.

- **Maturity of an Organisation**
  For many companies, embedding sustainability and ESG considerations within their organisations presents both a challenge and an opportunity. This means that often companies are at different levels of maturity when it comes to integrated business practices. This maturity can be measured, for example, by identifying where responsibility and accountability for sustainability sits within the organisation, the alignment between ESG material topics and risk factors, quality of ESG disclosure as well as governance mechanisms and processes.

- **The Evolving Regulatory and Voluntary Disclosure Landscape**

  New mandatory reporting standards are being driven by the increasing recognition by regulators and others for the need to build a common ground for disclosure to ensure effective communications of ESG-relevant information between corporates and investors. Capital markets need decision-useful and reliable information around companies' strategic sustainability risks and opportunities to understand their short, medium, and long-term value creation.

  In addition to climate-related financial disclosures, there is strong market momentum towards including "nature positive" in corporate disclosures.

- **Net-Zero and Nature-Positive Commitments**

  Companies need to consider how to embed action on climate and nature into their business practices and drive action down their supply chains. Commitments must be supported by coherent strategies with interim targets to measure progress. Governance structures and board responsibilities will need to be reconfigured to include more complex ESG information and corporate ESG disclosures will need to be transparent and have high levels of external assurance.

- **Pressure from Investors and Other Stakeholders**

  The board has a critical role to play in challenging management and should encourage the integration of financial and non-financial information so that stakeholders can be provided with investment grade data. But the board in its oversight role should look beyond the views of shareholders and consider its responsibility to understand stakeholder views firsthand to better inform boardroom decision-making.

- **Trust and Reputation**

  Building and maintaining trust and confidence with stakeholders is necessary to ensure that business and investor decision-making can rely upon the information.

  The broad and complex nature of sustainability topics means that organisations need to raise awareness and build capacity to ensure that multiple departments understand how the business could be impacted.

What should Internal Auditors do?

IPPF *Standard* 1100 – Independence and Objectivity stated that the internal audit activity must be independent, and internal auditors must be objective in performing their work.

Internal audit, independent from the governing body and the management, assures the reliability of internal control processes for ESG data disclosure and reporting.

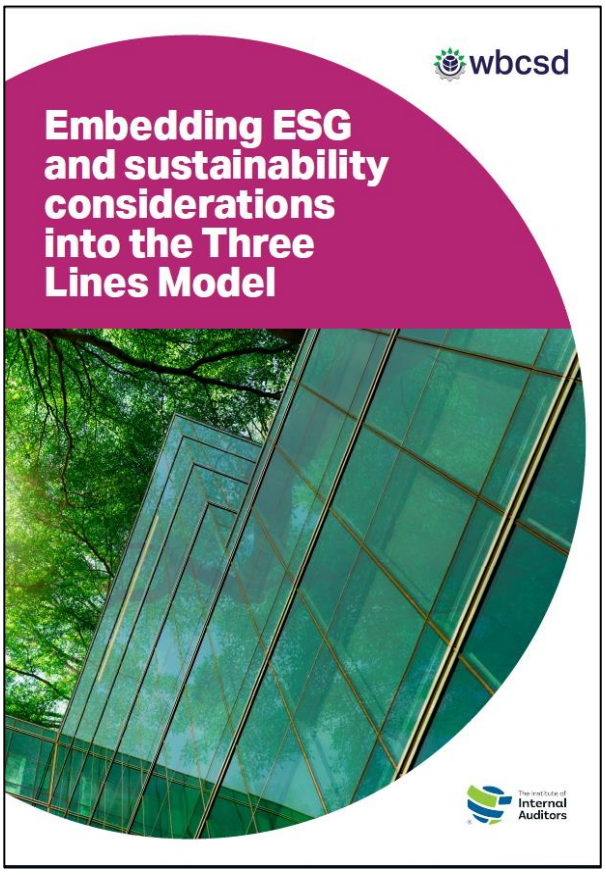
Internal audit is ideally placed to help companies evaluate opportunities, assess changes to operations and reporting, meet regulations, and be a catalyst for innovation and improvement for sustainability.

IPPF *Standard* 2300 – Performing The Engagement stated that internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

Internal auditors can test internal controls on ESG disclosure and assure that the ESG data are collected consistently to guarantee confidence in the data collection process. The internal control environment presents clear practices to ensure two-way communication and feedback loops between management and internal audit.

IPPF *Standard* 2500 – Monitoring Progress stated that the chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.

Internal auditors can monitor the evolving regulatory landscape and level of harmonisation between different regulatory frameworks.



Reference:
https://www.theiia.org/en/content/tools/advocacy/2022/embedding-esg-and-sustainability-considerations-into-the-three-lines-model/

GLOBAL KNOWLEDGE BRIEF

INTERNAL AUDIT IN A POST COVID WORLD - PART 1: TALENT MANAGEMENT (BY IIA GLOBAL)

- **Evolving Employee Expectations**

  As the pandemic's devastating impacts began to wane with isolation, development and distribution of effective vaccines, and the passage of time, employers eagerly sought a return to normality by bringing employees back to the office. However, determining just how — and how soon — to bring workers back has created considerable consternation, as survey after survey shows many employees are seeking flexibility from their employers, which includes working from home some or all of the time. This desire for a hybrid work option should not be viewed as synonymous with flexibility. Indeed, human resources experts say work-from-home options are just part of the growing demands from a workforce that is seeking greater understanding and support from their employers for a healthy work-life balance.

- **Technology and Talent**

  Numerous surveys and studies have noted the pandemic helped accelerate adoption of technology to increase efficiency and productivity. That adds a level of complexity to the post-COVID talent management risk. Organisations that fall behind in terms of technology will struggle to bring in top talent.

  The value of greater understanding of technology is manifesting clearly in the high turnover in financial services, where FinTech — the growing field where technology and innovation are altering delivery of traditional financial services — is drawing new and experienced workers. FinTech includes artificial intelligence, blockchain, cloud computing, and leveraging big data.

... 12

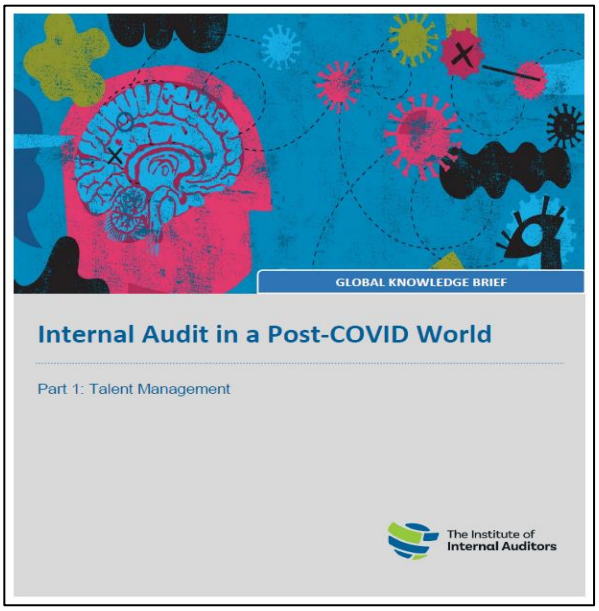
- **Diversity, Equity, and Inclusion**

  As organisations battle to adapt to changing worker demands on work-life balance and meeting new challenges and opportunities offered by technology, a third component to talent management in a post-COVID environment lies in what the organisation looks like. Diversity, equity, and inclusion presents a significant opportunity to attract and retain top talent.

What should Internal Auditors do?

IPPF *Standard* 1200 – Proficiency and Due Professional Care mentioned engagements must be performed with proficiency and due professional care.

Internal audit functions should be focusing instead on automating source systems to manage routine and repetitive chores, which then provides the opportunity to step back and identify potential roadblocks to the organisation achieving its goals.



Reference:
https://www.theiia.org/en/content/articles/global-knowledge-brief/2022/august/internal-audit-in-a-post-covid-world-part-1-talent-management/

GLOBAL KNOWLEDGE BRIEF

CYBERSECURITY IN 2022 - PART 3: CYBER INCIDENT RESPONSE AND RECOVERY (BY IIA GLOBAL)

Organisations desire, indeed, require, clear, robust cybersecurity controls and processes built on core fundamentals, including continuous learning about the risk and its related regulations, as well as communication and alignment among the board, management, and internal audit.

- **The Fallacy of Incident Response**

  Internal audit in its most essential role provides organisations with independent assurance over risk management. This includes not only assurance for appropriate response to cyber incidents, but also proper evaluation of controls to ensure that the risk and its effects are mitigated or, ideally, prevented. To attain such a lofty standard over any given risk, attention should not just be reserved for simply responding to a risk. Instead, it is more effective to view cyber incident response in a holistic, cyclical manner that prioritizes preventive controls as well as active response measures.

- **Unchanging Fundamentals**

  Risks seldom become less complex, and because cybersecurity is inherently highly technical, the learning curve to understand both the risk itself and the systems necessary to mitigate it have only grown steeper with every subsequent technological advancement. However, this does not necessarily mean that the fundamental structure of a cyber incident response plan, and the controls within it, change dramatically.

- **Documentation Controls**

  Organisations must understand what workflows look like that properly document cyber incidents, and how all the moving parts running in parallel.

- **Detection and Physical Infrastructure Controls**

  Another critical control, and one that falls under the rubric of unauthorised access risks, is physical infrastructure. Although such controls may not immediately come to mind when discussing cybersecurity, unauthorised access to hard drives or servers where sensitive information is stored was responsible for 10% of all malicious breaches in 2020.

  Such infrastructure can include secure server rooms with restricted access, as well as more basic security measures, such as locked doors throughout facilities. While infrastructure security is important, having controls in place to detect and document potentially suspicious activity can be more relevant.

- **Alignment of Recovery Expectations**

  Effective documentation in all stages of a cyber incident response plan is critical. Equally critical, however, is the communication of the data such documentation provides and the alignment of organisational detection and recovery expectations.

- **Cross-Functionality**

  It is a common misconception that primary ownership of cybersecurity response falls to the CISO and the security team. This is only partially true.

  Cyber incident response is, at least it should be, a cross-functional process. According to Ross, correcting this misconception and fostering the idea of shared responsibility across all stakeholders should be a key area of internal audit focus.

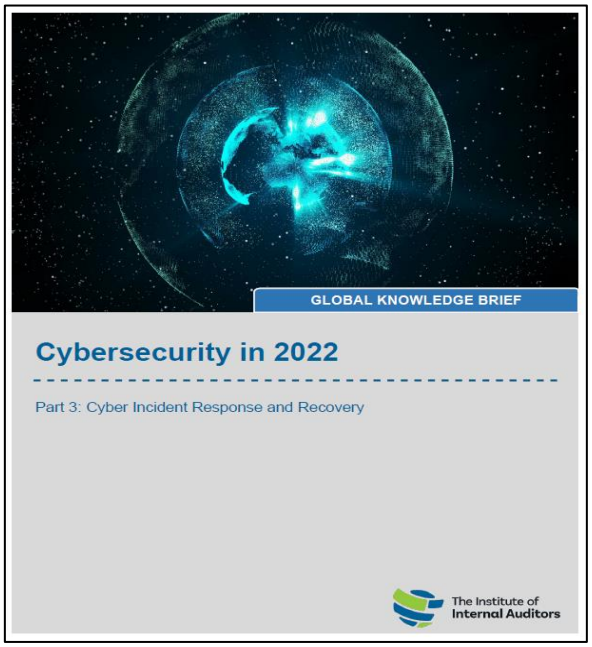
What should Internal Auditors do?

IPPF *Standard* 1200 – Proficiency and Due Professional Care mentioned engagements must be performed with proficiency and due professional care.

Internal auditors are not excused from striving for deeper exploration and understanding of cybersecurity. Indeed, in a future that is quickly dispensing with physical infrastructure in favor of cloud-based technology, greater expertise from internal audit will inevitably become necessary and expected. This includes not only assurance for appropriate response to cyber incidents, but also proper evaluation of controls to ensure that the risk and its effects are mitigated or, ideally, prevented.

IPPF *Standard* 2500 – Coordination and Reliance mentioned the chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimise duplication of efforts.

In this scenario, internal auditor can collaboration with an external consultant to facilitate tabletop simulations.



Reference:

https://www.theiia.org/en/content/articles/global-knowledge-brief/2022/july/Cybersecurity-Part-3-Cyber-Incident-Response-and-Recovery/

INTERNAL AUDIT 360

WHAT INTERNAL AUDIT GETS WRONG WHEN ASSESSING CYBERSECURITY RISK (BY NORMAN MARKS)

One of the challenges when it comes to so-called "cybersecurity risk" is in accepting and then applying the idea that cyber is not an "IT risk." No. It's a business risk. The truth is that cybersecurity must be seen within the context of the whole business, not in a silo.

If internal auditors want to assess the management of cybersecurity risk, they should take a more holistic approach, starting with the answers to the question: "What is the potential effect of a breach on the achievement of the enterprise's objectives?" An audit should probably include the participation of financial and operational auditors, and not be limited to the infosec experts.

If management has not completed and then maintained a business risk-oriented risk assessment that is integrated with enterprise risk management and decision-making, the audit team should consider calling the audit to a halt.

While the business cannot be considered absent IT-related risks and opportunities, those IT-related risks and opportunities cannot be considered absent the context of running the business and achieving objectives. Cyber (and other IT-related risks) should not be considered in a silo. Furthermore, cyber (and other IT-related risks) is just one source of risk that needs to be considered in decision-making.

In fact, a cyber incident can create a supply-chain, compliance, operational, financial, or other risk – because risk is inter-related. Similarly, a change in the supply chain such as the use of a new logistics company, or a change in operations or financial advisor, can change cybersecurity-related risks.

Cybersecurity risk assessment and treatment should be an integral part of the organisation's enterprise risk management program (ERM) and decision-making, not a siloed operation. If cybersecurity is not fully integrated, then Internal Audit should be reporting that to the board. We need to be concerned with risk to the ability of the organisation to achieve its objectives, its purpose over time.

What should Internal Auditors do?

IPPF *Standard* 1100 – Independence and Objectivity stated that the internal audit activity must be independent, and internal auditors must be objective in performing their work.

Internal auditors should provide their professional opinion on whether management's processes and controls provide reasonable assurance that there is a low (i.e., acceptable) likelihood of a breach with an unacceptable effect on the organisation and the achievement of its objectives.

Reference:

https://internalaudit360.com/what-internal-audit-gets-wrong-when-assessing-cybersecurity-risk/

If you missed out the previous issues of e-techline, you may visit our website at https://iiam.com.my/technical-qa-services/e-techline/.