

# AUDIT AND GOVERNANCE COMMITTEE



Report subject	<b>Internal Audit – Audit Plan 2025/26 Response to Queries</b>
Meeting date	29 May 2025
Status	Public Report
Executive summary	<p>At the Audit &amp; Governance Committee meeting on 20 March 2025, the approval of the 2025/26 Internal Audit Plan was deferred to the next meeting on 29 May 2025. The Committee requested clarification on nine points derived from the Institute of Internal Auditor's (IIA) Supplementary Guidance (non-mandatory) document "Developing a Risk Based Internal Audit Plan".</p> <p>This report responds to each point and clarifies the process followed by the BCP Internal Audit Function in determining its Internal Audit Plan and demonstrating conformance to the IIA's mandatory requirements of the International Professional Practices Framework 2024 (IPPF).</p> <p>The Chief Internal Auditor is satisfied that the Internal Audit team comply with all the mandatory elements of the IPPF (including the Global Internal Audit Standards and relevant application notes) and previously verified by external assessment.</p> <p>Internal Audit planning takes into account the non-mandatory guidance elements of the IPPF.</p> <p>Ensuring the Committee is equipped with all relevant, sufficiently detailed, information, to enable them to meaningfully consider and agree the Plan has continually evolved over time and requires judgement on what level of detail is helpful to the Committee. As a trial, further information has been included in the Internal Audit – Audit Plan 2025/26 report which is being brought separately to this Committee.</p>
Recommendations	<p><b>It is RECOMMENDED that Audit &amp; Governance Committee:</b></p> <p><b>a) Note the responses to the audit planning queries raised at the Audit &amp; Governance Committee on 20 March 2025</b></p>
Reason for recommendations	<p>To comply with the mandated Global Internal Audit Standards and Application Note: Global Internal Audit Standards in the UK public sector.</p>

Portfolio Holder(s):	Cllr Mike Cox, Deputy Leader of the Council, Vice-Chair of Cabinet and Cabinet Member for Finance
Corporate Director	Graham Farrant, Chief Executive
Report Authors	Nigel Stannard Head of Audit & Management Assurance ☎01202 128784 ✉ <a href="mailto:nigel.stannard@bcpcouncil.gov.uk">nigel.stannard@bcpcouncil.gov.uk</a> Ruth Hodges Deputy Chief Internal Auditor
Wards	Council-wide
Classification	For Information

## Background

1. At the Audit & Governance Committee meeting on 20 March 2025, the approval of the 2025/26 Internal Audit Plan was deferred to the next meeting on 29 May 2025. The Committee requested clarification on several points surrounding the internal audit planning process.
2. This report sets out to respond to each point raised by the Committee and to clarify the process followed by the BCP Internal Audit Function in determining its Internal Audit Plan and demonstrating conformance to the requirements of the Institute of Internal Auditor's International Professional Practices Framework 2024 (IPPF).
3. The IPPF guides the professional practice of internal auditing. It comprises of three components, the Global Internal Audit Standards (GIAS), Topical Requirements, and Global Guidance.



Mandatory	<p><b>Global Internal Audit Standards</b> guide the worldwide professional practice of internal auditing and serve as a basis for evaluating and elevating the quality of the internal audit function. At the heart of the Standards are 15 guiding principles that enable effective internal auditing. Each principle is supported by standards that contain requirements, considerations for implementation, and examples of evidence of conformance. Together, these elements help internal auditors achieve the principles and fulfill the Purpose of Internal Auditing.</p>
	<p><b>Topical Requirements</b> are designed to enhance the consistency and quality of internal audit services related to specific audit subjects and to support internal auditors performing engagements in those risk areas. Internal auditors must conform with the relevant requirements when the scope of an engagement includes one of the identified topics.</p> <p>Topical Requirements strengthen the ongoing relevance of internal auditing in addressing the evolving risk landscape across industries and sectors.</p>
Supplemental	<p><b>Global Guidance</b> supports the Standards by providing nonmandatory information, advice, and best practices for performing internal audit services. It is endorsed by The IIA through formal review and approval processes.</p> <p>Global Practice Guides provide detailed approaches, step-by-step processes, and examples on subjects including:</p> <ul style="list-style-type: none"> <li>• Assurance and advisory services.</li> <li>• Engagement planning, performance, and communication.</li> <li>• Financial services.</li> <li>• Fraud and other pervasive risks.</li> <li>• Strategy and management of the internal audit function.</li> <li>• Public sector.</li> <li>• Sustainability.</li> </ul> <p>Global Technology Audit Guides (GTAG®) provide auditors with the knowledge to perform assurance or consulting services related to an organization's information technology and information security risks and controls.</p>

*Extract from the "Global Internal Audit Standards" – published by the Institute of Internal Auditors (January 2024)*

- The diagram above shows the GIAS and Topical Requirements form the mandatory components of the IPPF, whilst the Global Guidance offers additional information, advice, and best practice for conducting internal audit services, and is a supplementary (non-mandatory) component.
- For the UK public sector, it has been mandated that the GIAS consists of both the GIAS and the Application Note: Global Internal Audit Standards in the UK Public Sector which interprets the GIAS requirements for the sector.

6. In addition, local authorities are expected to comply with CIPFA's Code of Practice for the Governance of Internal Audit in UK Local Government.
7. One of the independent members on the A&G committee raised a number of queries citing the "Developing a Risk Based Internal Audit Plan Supplemental Guidance - May 2020" document. This forms part of the wide suite of supplemental global guidance (part 3 in the diagram above) which is non-mandatory and parts of which are currently being updated to reflect the new standards (GIAS).
8. So, whilst this particular piece of supplementary guidance exists there are more relevant and focused UK public sector mandatory requirements as set out above.
9. In recent years, the Internal Audit profession has changed to a more dynamic Internal Audit Planning approach. Recent articles issued by professional journals include headlines such as "It's Time to Ditch the Annual Audit Plan" (April 2024 – Internal Audit 360) in which the author reflects:  
  
*"Sadly, though, many internal audit departments still undertake the annual process of conducting a once-a-year risk assessment in the fourth quarter and using it as the basis for the annual audit plan, which they follow, unwavering, for the next twelve months. Some CAEs (chief audit executives i.e. chief internal auditor) are even held accountable as part of their performance metrics to complete that annual plan, regardless of how circumstances and risks have changed through the year."*  
  
Colleagues in our professional networking groups are increasingly planning flexibly, with this reported in the IIA's Audit & Risk Magazine in May 2024 quoting *"Flexibility is key. When I started my career a three-year audit plan was normal. Then we moved to one-year and then to rolling plans"*
10. For context, the Developing a Risk Based Internal Audit Plan supplementary guidance states: "While the annual risk assessment is the minimum requirement articulated in the Standards, today's rapidly changing risk landscape demands that internal auditors assess risks frequently, even continuously. Risk-based internal audit plans should be dynamic and nimble. To achieve those qualities, some CAEs update their internal audit plan quarterly (or a similar periodic schedule), and others consider their plans to be rolling, subject to minor changes at any time".
11. The mandatory GIAS requirements regarding the Internal Audit Plan can be found at Appendix 1. BCP Council Internal Audit have undertaken a self-assessment against these standards and 'generally conforms' with them with an action plan in place to work towards full conformance (as reported to Audit & Governance Committee on 20 March 2025). The detailed extract from the GIAS, section 9.4 'Internal Audit Plan' is also included for information in Appendix 2.
12. The BCP Internal Audit function was externally assessed by an independent assessor (CIPFA) against the then Public Sector Internal Audit Standards (now superseded by the GIAS from April 2025) in June 2021 as reported to the committee on 28 October 2021. The external assessment concluded that the BCP Internal Audit function fully conformed with the PSIAS.
13. The external assessment process is required every five years, BCP Internal Audit's next external assessment, against the GIAS, will be in June 2026.

14. Internal Audit is confident that it complies with mandatory guidance and considers professional best practice when producing the Internal Audit plan.

### **Response to Audit & Governance Committee Queries**

15. An Independent member sought clarification on nine points derived from the IIA Supplementary Guidance (non-mandatory) – Developing a Risk Based Internal Audit Plan.
16. Ensuring the Committee is equipped with all relevant, sufficiently detailed, information, to enable them to meaningfully consider and agree the Plan, has continually evolved over time.
17. The level of detail reported to Committee is not pre-defined by the standards, inevitably this requires judgement on what level of detail is helpful to the Committee to make informed decisions versus what would be excessive, both in terms of the requirements of the Committee and in terms of resource required to produce.
18. More detail to support the Plan is produced but not all is reported to Audit & Governance Committee. Internal Audit is able to provide more information either on an ad-hoc or on-going basis if required.
19. The table below shows in the first column, the independent member's opinion/statement and in the second column Internal Audit's responses:

Column 1 - Independent member's comments – Note these are taken directly from the Developing a Risk Based Internal Audit Plan Supplementary guidance.	Column 2 - Internal Audit Response
The following is suggested to be included in the Internal Audit plan report to the Audit Committee:	
<p>Risk assessment summary</p> <ul style="list-style-type: none"> <li>Organizational strategy, key areas of focus, key risks, and associated assurance strategies in the audit plan.</li> <li>Summary of risks.</li> <li>Analyses (or summary) of inherent and/or residual risk levels of auditable units.</li> <li>Risk scores/ratings for auditable units.</li> <li>Heat map for entire audit universe indicating priorities, inclusions, and exclusions.</li> </ul> <p><i>Independent member's Opinion/Statement – The auditable areas are listed on page 265 of the agenda pack; however these areas are not linked to risks. According to the International Auditing Standards an Internal audit plan should be risk based. There is no clear correlation between auditable units and risk.</i></p>	<p>Please note that the guidance document “<i>Risk assessment summary – A description of the risk assessment process and results enhances the board’s understanding of internal audit’s priorities. Information may include...</i>”</p> <p><b>Risk Based Approach</b></p> <p>Internal Audit’s Risk Assessment Process was reported to the Audit &amp; Governance Committee on 27 January 2025, paragraph 15. This includes risk assessments against organisational strategy and key risks.</p> <p>Whilst risks for individual engagements are not reported to the Committee, risk assessments are carried out and documented within the Audit Management System including a risk rating for all audits within audit universe.</p> <p>The information, including risk ratings, within the Audit Management System is used to produce the plan.</p> <p>As a trial, the Quarterly Plan, which is being brought separately to this Committee, will include the Internal Audit Risk Score, Reason for Inclusion, Link to Corporate / Service Risk and Link to Corporate Strategy (as well as date last audited). In that report, the Committee will be asked to consider whether the additional information is helpful and wish to continue to receive it at future committees.</p>

Column 1 - Independent member's comments – Note these are taken directly from the Developing a Risk Based Internal Audit Plan Supplementary guidance.	Column 2 - Internal Audit Response
<p>A list of proposed audit engagements (and specification regarding whether the engagements are assurance or consulting in nature).</p> <p><i>Independent member's Opinion/Statement – the Internal Audit plan list the proposed audit engagements, however, does not indicate whether the engagements are assurance or consulting in nature.</i></p>	<p>Internal Audit carry out non-assurance (advisory services<sup>1</sup>) work, under the headings of “Investigations, advice, financial regulation compliance” on the Internal Audit Plan, which is reported to Committee.</p> <p>The audits detailed within the proposed Internal Audit Plan are all deemed to be “Assurance” engagements in nature unless otherwise stated.</p> <p>There are rare occasions where a proposed assurance review changes to an advisory/consultancy review during the detailed scoping. Such instances will be clearly highlighted, with an explanation, within the quarterly report to each committee.</p>
<p>Tentative scopes and objectives of audit engagements.</p> <p><i>Independent member's Opinion/Statement – the Internal Audit plan list the proposed audit engagements as headings only. Tentative scopes and objectives of audit engagements not documented.</i></p>	<p>The risk assessment and annual planning process, including discussions with senior management, helps to determine the likely coverage of the audit. However, detailed scoping is carried out immediately prior to commencement of the audit to take account of the current risks facing the service. This is also an efficient use of Audit resource, so time is not spent scoping an audit which may not be undertaken or where changes result in amendments to the scope.</p> <p>Note the new Reason for Inclusion column on the Quarterly Plan will include some information regarding the scope.</p> <p>In conclusion, scoping of audit engagement is carried out prior to the commencement of the audit to reflect that Internal Audit operate a rolling audit plan and for purposes of operational efficiency. (note paragraph 9 above).</p>
Tentative timing and duration (timeline showing the quarter during which the	Internal Audit has an operational plan that is not reported to

<sup>1</sup> **Advisory Services** – Services through which internal auditors provide advice to the Council without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. “Advisory services” are also known as “consulting services.”

Column 1 - Independent member's comments – Note these are taken directly from the Developing a Risk Based Internal Audit Plan Supplementary guidance.	Column 2 - Internal Audit Response
<p>engagement will be performed and how long it will take to complete).</p> <p><i>Independent member's Opinion/Statement – the Internal Audit plan includes anticipated days, but not the quarter the audits are to be performed.</i></p>	<p>committee, this is a management tool that broadly identifies, by quarter, when audits may be performed. This is subject to significant change to take account of competing priorities/risk/resources.</p> <p>Detailed audit planning is undertaken on a quarterly basis and the Committee is provided with the proposed audits for the next quarter.</p> <p>Paragraph 9 described the audit profession is moving away from the production of detailed annual plans.</p>
<p>Assurance coverage and exclusions – This section may include an assurance map, summary, or other tool to communicate assurance coverage over significant risk areas. Exclusions acknowledge auditable units or risk areas that are not addressed, and if any high-risk areas are not covered (e.g., due to resource limitations), then this section may include recommendations to the board for obtaining assurance, such as via co-sourcing or outsourcing.</p> <p><i>Independent member's Opinion/Statement – see point 1 above, as risks are not linked to proposed auditable area, reasons cannot be given if high risk areas are not covered.</i></p>	<p>As part of the audit planning process, Internal Audit consider all of the Council's high-risk area as identified in the Corporate Risk register. In addition, the audit planning process includes assurance mapping, which was reported to Committee in Appendix A of the Internal Audit – Audit Plan 2025/26 report.</p> <p>Internal Audit report exclusions from the approved operational Internal Audit Plan in the quarterly updates to Committee as required.</p>
<p>Rationale for inclusions and exclusions – This explanation is important, especially if risk ratings or frequency determinations are overridden. Reasons may include change in risk rating, length of time since last audit, change in management, and more.</p> <p><i>Independent member's Opinion/Statement – Rationale for inclusions and exclusions of proposed auditable areas not provided.</i></p>	<p>The rationale for inclusions on the Internal Audit Plan is based on the Internal Audit Risk Assessment process which includes the date of the previous audit review. Reason for inclusion and date last audited will be included on the proposed Quarterly Plan as a trial as stated above.</p> <p>Reasons for excluding audits from the initial operational audit plan are due to risk scores, date last audited, ensuring assurance is obtained across the organisation, availability of other reliable</p>



Column 1 - Independent member's comments – Note these are taken directly from the Developing a Risk Based Internal Audit Plan Supplementary guidance.	Column 2 - Internal Audit Response
	<p>sources of assurance, and total resource available to the Internal Audit team. With over 500 audits in the audit universe, the Chief Internal Auditor does not consider that it would be meaningful to report individually on reasons for exclusions from the operational audit plan, nor an appropriate use of Internal Audit resource to produce such a report. As noted above, where audits are excluded from the operational audit plan, these are reported to Committee.</p> <p>Note that given the move towards dynamic audit planning, frequency is no longer predetermined for many auditable areas in the audit universe, instead, coverage is determined as part of the risk assessment process. However, the Key Assurance Functions and Key Financial Systems are reviewed annually and Maintained Schools every three years. Any deviation from this would be reported to the Committee.</p>
<p>Resource plan – This section identifies the type and quantity of resources that will be needed to execute the plan. The description may include the number of staff required to complete the audit plan (capacity), the number of support staff needed, a summary of the results of the skills assessment, and a plan of action to address skill gaps.</p> <p><i>Independent member's Opinion/Statement - Paragraph 15 on page 260 of the audit pack states: 'The allocated budget resource for 2025/26 is considered adequate to deliver the Internal Audit Charter 2025 and 2025/26 Audit Plan. Audit &amp; Governance Committee are asked to note the budget for the Internal Audit service which has been previously approved by Council as part of the 2025/26 Budget setting and Medium Term Financial Plan update in February 2025.</i></p> <p><i>The internal audit plan confirms that the capacity of the IA unit is sufficient, however does not address the results of the skills assessment or has a plan</i></p>	<p>The Chief Internal Auditor considers that this is undertaken and appropriately reported to Committee. The Chief Internal Auditor's annual report, annual audit plan reports and quarterly reports state the staff resource available together with a statement that the Chief Internal Auditor considers this sufficient.</p> <p>The known specialist ICT audit in-house skills gap has been proactively addressed through external sourcing (circa 10 days) for a number of years, as per the Audit Charter. When staff resources are not considered sufficient, the resultant action plan is reported to Committee, for example, the recruitment of apprentices to address recruitment issues in the Quarterly Report in July 2023.</p>

Column 1 - Independent member's comments – Note these are taken directly from the Developing a Risk Based Internal Audit Plan Supplementary guidance.	Column 2 - Internal Audit Response
<p><i>of action to address skill gaps.</i></p>	
<p>Financial budget requirements – The plan includes a financial budget to cover payroll of internal audit staff, as well as the cost of cosourced and/or outsourced services, tools (i.e., technology), training, and other expenses.</p> <p><u><i>Independent member's Opinion/Statement</i></u> - The plan includes the anticipated staff audit days and a total amount for the IA financial payroll as budgeted. The plan does not make mention of cosourced and/or outsourced services, tools (i.e., technology), training, and other expenses.</p>	<p>The Chief Internal Auditor considers that reporting to Committee for financial budget area is adequate. The latest report states “The BCP Internal Audit Team budgeted cost for 2025/26 is £776,000. This budget is inclusive of all direct costs including supplies and services but does not include the apportionment of central support costs (which are budgeted in aggregate and apportioned to services as a separate exercise).” For clarity, this includes staffing costs (internal and external), ICT and other expenses.</p> <p>Training budgets are managed as part of the Financial Services wide budget and allocated following consideration of business cases.</p> <p>As per the Audit Charter, the Chief Internal Auditor is required to report any resource concerns that may impact upon the delivery of the annual audit opinion to the Chief Financial Officer and to this Committee.</p>
<p>Approval sign-off area – Senior management and the board must approve the plan.</p> <p><u><i>Independent member's Opinion/Statement</i></u> - The plan should be physically signed off by the relevant parties.</p>	<p>Senior Management on a directorate level agree the Internal Audit Plan. The Committee formally approve the Internal Audit Plan through the democratic process annually. There is no requirement for a physical sign-off of the Internal Audit Plan within the GIAS or supplementary guidance.</p> <p>The plan is approved as per the requirements of the GIAS.</p>

## **Options Appraisal**

20. Not required as part of this report.

## **Summary of financial implications**

21. Financial implications of the Internal Audit Plan are reported in a separate report to Committee.

## **Summary of legal implications**

22. Where the Internal Audit Plan is not approved by the Audit & Governance Committee, this risks the Council failing to adhere to Regulation 5 of the Accounts and Audit Regulations 2015 which requires the Council to “undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, and taking into account public sector internal auditing standards or guidance”.

## **Summary of human resources implications**

23. Human resources implications of the Internal Audit Plan are reported in a separate report to Committee.

## **Summary of sustainability impact**

24. There are no direct sustainability impact implications from this report.

## **Summary of public health implications**

25. There are no public health implications from this report.

## **Summary of equality implications**

26. There are no direct equality implications from this report.

## **Summary of risk assessment**

27. This report ensures compliance with the Global Internal Audit Standards and Application Note for the public sector.

## **Background papers**

Global Internal Audit Standards

CIPFA Application note: Global Internal Audit Standards in the UK Public Sector

IIA IPPF Supplemental Guidance – Developing A Risk Based Internal Audit Plan

## **Appendices**

Appendix 1 – Compliance with GIAS – relevant to audit planning

Appendix 2 – Extract from the Global Internal Audit Standards

## Compliance with GIAS – relevant to audit planning

GIAS Requirements	How BCP Internal Audit Comply
<b>Note – the Internal Audit Charter (as agreed by Audit &amp; Governance Committee) outlines how all the requirements of the GIAS are complied with</b>	
<b>Standard 8.1 Board Interaction</b>	
<b>Requirements</b>	
<p>The chief audit executive must report to the board and senior management:</p> <ul style="list-style-type: none"> <li>• The internal audit plan and budget and subsequent significant revisions to them.</li> </ul>	<p>The Internal Audit Plan is reported to Audit &amp; Governance Committee, annually in January and March/April, and an update, showing all revisions, is taken quarterly.</p>
<b>Essential Conditions</b>	
<b>Board</b>	
<ul style="list-style-type: none"> <li>• Communicate the board's perspective on the organization's strategies, objectives, and risks to assist the chief audit executive with determining internal audit priorities.</li> </ul>	<p>Consultation with the Audit &amp; Governance Committee is undertaken annually as part of the audit planning process. A&amp;G Committee can, and do, communicate concerns, in response to both Internal Audit reports, regular update reports from other functions or as a result of special reports.</p>
<b>Senior Management</b>	
<ul style="list-style-type: none"> <li>• Communicate senior management's perspective on the organization's strategies, objectives, and risks to assist the chief audit executive with determining internal audit priorities.</li> </ul>	<p>Senior management are consulted as part of the annual audit planning process.</p>
<b>Standard 9.4 Internal Audit Plan</b>	
<b>Requirements</b>	
<p>The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives.</p>	<p>The Internal Audit Plan is produced annually and updated during the year in response to changing risks. It is based on risks identified from a range of sources* including the Council's Corporate Strategy which articulates the Council's vision and</p>

	<p>ambitions (objectives) and corporate and service risk registers.</p> <p><small>** These can be found in the Audit Charter Appendix E</small></p>
<p>The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually.</p>	<p>The annual Internal Audit Planning process considers the Council's strategies, objectives and risks and the audit team's understanding of the governance, risk management and control processes (as shown in Appendix E of the Charter), and is informed by input from senior management and Audit &amp; Governance Committee.</p>
<p>The internal audit plan must:</p> <ul style="list-style-type: none"> <li>• Consider the internal audit mandate and the full range of agreed-to internal audit services.</li> <li>• Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.</li> <li>• Consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.</li> <li>• Identify the necessary human, financial, and technological resources necessary to complete the plan.</li> <li>• Be dynamic and updated timely in response to changes in the organization's business, risks operations, programs, systems, controls, and organizational culture.</li> </ul>	<p>The Internal Audit Plan reflects the mandate agreed as part of the Internal Audit Charter. It includes consideration of the areas identified, however, we have an action to ensure that ethics is more specifically identified as part of the process. Resources required are identified. The plan is updated throughout the year and the resultant changes reported to Audit &amp; Governance Committee quarterly.</p>
<p>The chief audit executive must review and revise the internal audit plan as necessary and communicate timely to the board and senior management:</p> <ul style="list-style-type: none"> <li>• The impact of any resource limitations on internal audit coverage.</li> <li>• The rationale for not including an assurance</li> </ul>	<p>Audit plan is reviewed and revised throughout the year and reported to Audit &amp; Governance in the quarterly reports. All points would be included if relevant.</p>

<p>engagement in a high-risk area or activity in the plan.</p> <ul style="list-style-type: none"> <li>• Conflicting demands for services between major stakeholders, such as high-priority requests based on emerging risks and requests to replace planned assurance engagements with advisory engagements.</li> <li>• Limitations on scope or restrictions on access to information.</li> </ul>	
<p>The chief audit executive must discuss the internal audit plan, including significant interim changes, with the board and senior management. The plan and significant changes to the plan must be approved by the board.</p>	<p>All changes to the Internal Audit Plan are agreed with the relevant senior management and reported to Audit &amp; Governance Committee quarterly.</p>

**Extract from the Global Internal Audit Standards - published by the Institute of Internal Auditors (January 2024)**

## Standard 9.4 Internal Audit Plan

### Requirements

The chief audit executive must create an internal audit plan that supports the achievement of the organization's objectives.

The chief audit executive must base the internal audit plan on a documented assessment of the organization's strategies, objectives, and risks. This assessment must be informed by input from the board and senior management as well as the chief audit executive's understanding of the organization's governance, risk management, and control processes. The assessment must be performed at least annually.

The internal audit plan must:

- Consider the internal audit mandate and the full range of agreed-to internal audit services.
- Specify internal audit services that support the evaluation and improvement of the organization's governance, risk management, and control processes.
- Consider coverage of information technology governance, fraud risk, the effectiveness of the organization's compliance and ethics programs, and other high-risk areas.
- Identify the necessary human, financial, and technological resources necessary to complete the plan.
- Be dynamic and updated timely in response to changes in the organization's business, risks operations, programs, systems, controls, and organizational culture.

The chief audit executive must review and revise the internal audit plan as necessary and communicate timely to the board and senior management:

- The impact of any resource limitations on internal audit coverage.
- The rationale for not including an assurance engagement in a high-risk area or activity in the plan.
- Conflicting demands for services between major stakeholders, such as high-priority requests based on emerging risks and requests to replace planned assurance engagements with advisory engagements.
- Limitations on scope or restrictions on access to information.

The chief audit executive must discuss the internal audit plan, including significant interim changes, with the board and senior management. The plan and significant changes to the plan must be approved by the board.

## Considerations for Implementation

This standard requires an organizationwide risk assessment to be completed at least annually as the basis for the plan. However, the chief audit executive should keep continuously apprised of risk information, updating the risk assessment and internal audit plan accordingly. If the organization's environment is dynamic, the internal audit plan may need to be updated as frequently as every six months, quarterly, or even monthly. The size, complexity, and type of changes occurring in the organization relative to the maturity of the organization's governance, risk management, and control processes should be considered when determining the appropriate level of effort to update the risk assessment.

One approach to preparing the internal audit plan is to organize potentially auditable units within the organization into an audit universe to facilitate the identification and assessment of risks. An audit universe is most useful when it is based on an understanding of the organization's objectives and strategic initiatives and aligned with the organization's structure or risk framework. Auditable units may include business units, processes, programs, and systems. The chief audit executive can link those organizational units to key risks in preparation for a comprehensive risk assessment and the identification of assurance coverage throughout the organization. This process enables the chief audit executive to prioritize the risks to be evaluated further during internal audit engagements.

To strive to ensure that the audit universe and risk assessment cover the organization's key risks, the internal audit function should independently review and validate the key risks that were identified within the organization's risk management system. The internal audit function should only rely on management's information about risks if it has concluded that the organization's risk management processes are effective.

To complete the organizationwide risk assessment, the chief audit executive should consider objectives and strategies not just at the broad organizational level but also at the level of specific auditable units. Additionally, the chief audit executive should give due consideration to risks — such as those related to ethics, fraud, information technology, third-party relationships, and noncompliance with regulatory requirements — that may be tied to more than one business unit or process and may require more complex evaluation.

To support this risk assessment, the chief audit executive may gather information from recently completed internal audit engagements as well as discussions with members of the board and senior management. (See also Standards 9.1 Understanding Governance, Risk Management, and Control Processes and 11.3 Communicating Results.) The chief audit executive may implement a methodology for continuously assessing risks. Risks should be considered not only in terms of negative effects and barriers to achieving objectives but also in terms of opportunities that enhance the organization's ability to achieve its objectives.

The chief audit executive should develop a process to identify and assess significant, new, and emerging risks that should be considered for coverage in the audit plan. For example, resource limitations may make it impossible for the internal audit function to assess every risk in the audit universe annually. In such cases, the chief audit executive may need to increase reliance on sources of risk information such as management's risk assessments, meetings with the board and senior management, and the results of previous engagements and other audit work.

To create the internal audit plan, the chief audit executive considers the level of risk identified across each of the auditable units relative to the known level of control effectiveness. Also influencing the internal audit plan are requests made by the board and senior management, the assurance coverage expected throughout the organization, engagements required by laws or regulations, and the internal audit function's ability to rely on the work of other assurance providers. The chief audit executive should plan to reevaluate reliance periodically.



When developing the internal audit plan, the chief audit executive should consider the following:

- Engagements required by laws or regulations.
- Engagements critical to the organization's mission or strategy.
- Areas and activities with significant levels of risk.
- Whether all significant risks have sufficient coverage by assurance providers.
- Advisory and ad hoc requests.
- The time and resources required for each potential engagement.
- Each engagement's potential benefits to the organization, such as the engagement's potential to contribute to the improvement of the organization's governance, risk management, and control processes.

To schedule internal audit engagements, the chief audit executive should consider:

- The organization's operational priorities.
- Schedule of external audit engagements and regulatory reviews.
- Competencies and availability of internal auditors.
- Ability to access the activity under review.

The proposed internal audit plan should include:

- The resources and hours available for engagements compared to other administrative and nonaudit activities or initiatives focused on improving the internal audit function.
- The list of proposed engagements and related analysis, specifying the degree to which the engagements are:
  - Assurance or advisory.
  - Focused on certain departments, units, or objectives of the organization.
  - Predominately addressing financial, compliance, operational, cybersecurity, or other objectives.
- The rationale for selecting each proposed engagement; for example, significance of risk, organizational theme or trend (root cause), regulatory requirement, or time since last engagement.
- General purpose and preliminary scope of each proposed engagement.
- A percentage of hours to be reserved for contingencies and ad hoc requests.
- The next set of engagements that would have been performed if additional resources were available. Discussion regarding these engagements may help the board assess the adequacy of resources available to the internal audit function.

The chief audit executive, the board, and senior management should agree upon the criteria that define the significant changes that require a revision of the audit plan. The agreed-upon criteria and protocol should be incorporated into the internal audit function's methodologies. Examples of significant changes include canceling or postponing engagements related to significant risks or critical strategic objectives. If risks arise that necessitate revisions to the plan before a formal discussion with the board can be scheduled, the board should be informed of the changes immediately, and a formal approval should occur as soon as possible.

## Examples of Evidence of Conformance

- Approved internal audit plan.
- Documented risk assessment and prioritization, including the inputs upon which the plan is based.
- Minutes of meetings in which the chief audit executive discussed with the board and senior management the audit universe, organizationwide risk assessment, internal audit plan, and the criteria and protocol for handling significant changes to the plan.
- Notes documenting discussions to gather information to inform the organizationwide risk assessment and internal audit plan.
- Documented list of those to whom the internal audit plan was distributed.
- Documented methodologies for organizationwide risk assessment and protocol for handling significant changes.