



## INTERNAL AUDIT ASSESSMENT CRITERIA<sup>1</sup>

### ROLE OF INTERNAL AUDIT

The Internal Audit function provides to the Board of Directors (through the Audit Committee) and Senior Management of a federally-regulated financial institution (institution) independent assurance of the effectiveness of, and adherence to, the institution's internal control, risk management and governance processes.

Under OSFI's Supervisory Framework and the 'three lines of defence' model:

- First line management (the 1<sup>st</sup> line of defence) are responsible for maintaining effective internal controls (policies, procedures and personnel) and risk management processes to manage risks and contribute towards achievement of the institution's objectives on a day-to-day basis;
- The independent, enterprise-wide oversight functions (the 2<sup>nd</sup> line of defence), including the Financial, Compliance, Actuarial and Risk Management functions (and Senior Management where they retain oversight responsibility) are responsible for helping build, and for monitoring the effectiveness of, 1st line management's internal control and risk management processes; and
- The Internal Audit function (the 3rd line of defence) provides the Board and Senior Management with assurance of the effectiveness of the internal control, risk management and governance processes used by the 1st and 2nd lines of defence and corporate governance functions based on the highest level of independence and objectivity within the institution. Internal Audit also may provide consulting services and advice on ways to improve processes.
- The Board and Senior Management (or 'corporate governance') are responsible for setting objectives and a risk appetite for the institution, defining strategies to achieve those objectives within the risk appetite, and establishing governance structures and processes to manage the risks in accomplishing those objectives.

### QUALITY OF INTERNAL AUDIT OVERSIGHT

The following statements describe the rating categories for the assessment of the Internal Audit function.

An overall rating of the Internal Audit function considers both the appropriateness of its characteristics and the effectiveness of its performance in executing its mandate, in the context of the nature, size, complexity, and risk profile of the institution. Characteristics and examples of performance indicators that guide supervisory judgment in determining an appropriate rating are set out below.

#### **Strong**

The characteristics of the Internal Audit function meet or exceed supervisory expectations of what is considered necessary, given the nature, size, complexity, and risk profile of the institution. Internal Audit characteristics and performance are superior to supervisory expectations.

<sup>1</sup> The Assessment Criteria should be read in conjunction with OSFI's Supervisory Framework and guidelines.



<b>Acceptable</b>
The characteristics of the Internal Audit function meet what is considered necessary, given the nature, size, complexity, and risk profile of the institution. Internal Audit characteristics and performance meet supervisory expectations.
<b>Needs Improvement</b>
The characteristics of the Internal Audit function generally meet what is considered necessary, given the nature, size, complexity, and risk profile of the institution, but there are some significant areas that require improvement and may affect effectiveness in the future or under adverse conditions. Internal Audit performance has generally been effective, but there are some significant areas where effectiveness needs to be improved. The areas needing improvement are not serious enough to cause prudential concerns if addressed in a timely manner. Internal Audit's characteristics and/or performance do not consistently meet supervisory expectations. .
<b>Weak</b>
The characteristics of the Internal Audit function are not, in a material way, what is considered necessary, given the nature, size, complexity, and risk profile of the institution and may affect effectiveness in the future or under adverse conditions. Internal Audit characteristics and/or performance often do not meet supervisory expectations..

<b>INTERNAL AUDIT CHARACTERISTICS<sup>2</sup></b>	
The following criteria describe the characteristics OSFI uses in assessing the quality of the Internal Audit function's independent assurance to the Board and Senior Management of the effectiveness of, and adherence to, the institution's internal control, risk management and governance processes. The application and weighting of the individual criteria will depend on the nature, size, complexity, and risk profile of the institution and will be assessed collectively, together with the Internal Audit function's performance, in rating its overall quality.	
<b>Essential Elements</b>	<b>Criteria</b>
<b>1. Mandate</b>	<p>1.1 Extent to which the function's mandate (may also be referred to as a 'charter') establishes:</p> <ul style="list-style-type: none"> <li>a) Clear objectives and responsibilities for the function and the Chief Internal Auditor (CIA);</li> <li>b) Enterprise-wide authority that encompasses all of the institution's operations, including all legal entities, operations in foreign jurisdictions, and activities that are outsourced. Its authority should encompass the internal control, risk management and governance processes used by the institution's 1<sup>st</sup> and 2<sup>nd</sup> lines of defence and corporate governance functions;</li> <li>c) Authority to carry out its responsibilities independently of the audited entities. The function should be free of any conflicts of interest or undue influence of the management of the audited entities or by the institution's Senior Management. The function should also not be directly involved in the management, decision-making or execution of the activities it audits;</li> <li>d) Right of access to the institution's records, information and personnel;</li> <li>e) A requirement to opine on the effectiveness of, and adherence to, the institution's internal control, risk management and governance processes. This includes (but is not limited to) opining on regulatory or prudential matters, such as: capital and liquidity management processes; Risk Appetite Framework design and processes; technology processes; strategic planning processes; etc., and</li> <li>f) Authority to follow-up with management on action taken in response to audit findings and recommendations.</li> </ul>
	1.2 Extent to which the function's mandate is communicated within the institution.

<sup>2</sup> Examples of documentation that OSFI may review in formulating its assessment of the characteristics of the Internal Audit function include: the curricula vitae of staff, professional training programs; Internal Audit mandates, manuals, work plans and audit reports and relevant materials discussed with the Audit Committee and Senior Management, and follow-up documentation related to audit findings; self-assessment reviews; and audit working papers.

<b>2. Organization Structure</b>	2.1 Appropriateness of the stature, access and authority of the CIA within the organization to challenge, and not be unduly influenced by, management of the activities it is responsible for auditing, as well as the institution's Senior Management. Although there may be some variations in reporting structure from institution to institution depending on the institution's nature, size and complexity, ideally, the CIA will report administratively to the CEO, and functionally to the Board (the Audit Committee). OSFI expects the CIA to be at the Senior Management level or the equivalent, and the heads of Audit for subsidiaries, branches and divisions to be comparable in seniority to the Senior Management of those entities. The CIA should be able to attend and observe Executive Committee meetings.
	2.2 Appropriateness of the function's organization structure for it to be effective in fulfilling its mandate, including the extent to which its activities are housed entirely within the institution (versus outsourced).
	2.3 Extent to which the function is organizationally independent of activities it audits and is not directly involved in the management, decision-making or execution of activities it audits.
<b>3. Resources</b>	3.1. Adequacy of the function's processes to determine the required: <ul style="list-style-type: none"> <li>a) Level of resources necessary to carry out responsibilities and in response to changes in the institution's business activities and strategies, as well as its operating environment;</li> <li>b) Qualifications and competencies of staff; and</li> <li>c) Continuing professional development programs to enhance staff competencies.</li> </ul>
	3.2. Adequacy of the function's resources and appropriateness of its collective qualifications and competencies for executing its mandate.
	3.3. Sufficiency of staff development programs.
<b>4. Audit Methodology and Practices</b>	4.1 Adequacy of the function's policies and practices to ensure that audit methodologies conform, as appropriate, to generally accepted industry practices and current professional standards (including the Institute of Internal Auditors standards).
	4.2 Appropriateness of audit methodologies and practices to execute the function's mandate.
	4.3 Extent to which the function's audit methodology is risk-based.
<b>5. Planning</b>	5.1 Extent to which the annual audit planning process is based on a robust risk assessment and provides appropriate coverage over a reasonable time period.
	5.2 Adequacy of policies and practices to review audit cycles and risk assessments regularly in order to proactively respond to changes in the institution's environment, risk profile and strategy.
	5.3 Extent to which the annual audit planning process clearly identifies audit objectives and scope of planned upcoming audits.
<b>6. Reporting</b>	6.1. Adequacy of policies and practices to report significant audit findings and recommendations to management so that timely corrective actions can be taken.
	6.2. Adequacy of policies and practices to monitor and follow-up on the effective implementation of management actions in response to audit findings and recommendations.
<b>7. Quality Assurance and Improvement</b>	7.1 Adequacy of a quality assurance and improvement program (QAIP) that: <ul style="list-style-type: none"> <li>a) Encompasses all of the function's activities (i.e., planning; resourcing; executing and reporting on audits; interacting with institution Senior Management and the Board (or Audit Committee), etc.);</li> <li>b) Assesses the efficiency and effectiveness of these activities, and makes appropriate improvements; and</li> <li>c) Monitors audit staff to ensure that they comply with professional standards and utilize approved methodology in executing their reviews.</li> </ul>

	7.2 Extent to which the functions's policies and practices ensure sufficient independence of the QAIP processes from the function's other activities.
<b>8. Relationship with 2<sup>nd</sup> Line of Defence Oversight Functions</b>	8.1 Extent to which the function assesses the institution's 2 <sup>nd</sup> line of defence oversight functions, and the adequacy and effectiveness of their processes, in order to be able to use their work and minimize duplication of efforts, where appropriate.
	8.2 Extent to which the function shares information and coordinates activities with 2 <sup>nd</sup> line of defence oversight functions to ensure proper coverage and integration of methodologies, and to minimize duplication of efforts.
<b>9. Senior Management Oversight</b>	9.1 Adequacy of policies and practices for Senior Management to support the Board (or Board Committee) on the: <ul style="list-style-type: none"> <li>a) Appointment and/or removal, performance review, compensation and succession plan of the function head;</li> <li>b) Function's mandate, budget and resources (staffing and skill sets); and</li> <li>c) Function's annual work plan including any material changes to that plan.</li> </ul>
	9.2 Adequacy of policies and practices to assess the effectiveness of the function, including communicating results to Senior Management and, as appropriate, the Board (or a Board committee).
	9.3 Adequacy of policies and practices to report periodically to Senior Management on issues and recommendations with escalation to the Board, as appropriate.
	9.4 Adequacy of the processes related to talent development and succession planning for function key roles.
<b>10. Board (and Audit Committee) Oversight</b>	10.1 Adequacy of policies and practices for the Board (or Board Committee) to approve: <ul style="list-style-type: none"> <li>a) The appointment, performance review, compensation and succession plan of the head of the oversight function;</li> <li>b) The function's mandate, budget and resources (staffing and skill sets); and</li> <li>c) The function's annual work plan including any material changes to that plan.</li> </ul>
	10.2 Extent to which the Board (or Board Committee) receives periodic reporting on trends or pervasive risk impacting the organization.
	10.3 Extent to which the Board (or Board Committee) demonstrates an ability to act independently of Senior Management through practices such as regularly scheduled Board (or Board Committee) meetings that include sessions without Senior Management present.

## INTERNAL AUDIT PERFORMANCE

The quality of the Internal Audit function's performance is demonstrated by its overall effectiveness in providing to the Board and Senior Management independent assurance of the effectiveness of, and adherence to, the institution's internal control, risk management and governance processes.

The assessment will consider how well the Internal Audit function promotes a sound control environment that mitigates risks, ensures that control weaknesses are appropriately dealt with, and provides the Board and Senior Management with assurance of the effectiveness of, and adherence to, internal control, risk management and governance processes. OSFI will look to indicators of effective performance to guide its judgement in the course of its supervisory activities. These activities may include:

- a) discussions with directors, management (including the CIA and heads of other oversight functions), and external auditors;
- b) review of how significant audit findings and management's responses to them are addressed with the Audit Committee;
- c) assessment of Internal Audit practices, reporting and outputs of its QAIP;
- d) review of audit plans and working paper files, etc.

Examples of indicators that could be used to guide supervisory judgement include the extent to which Internal Audit:

- a) Is viewed by the Audit Committee and Senior Management as being effective in executing its mandate;
- b) Regularly engages the Audit Committee on the continued appropriateness of the Internal Audit budget, resources (staffing and skill sets) and plan;
- c) Proactively communicates to the Audit Committee significant and persistent findings and management's action related to them;
- d) Reviews objectives, strategies, events, initiatives and transactions for changes that could materially impact the institution in order to ensure internal control, risk management and governance processes continue to be appropriate and effective;
- e) Actively seeks information from Risk Management, the Appointed Actuary, Compliance officers, external auditors, OSFI, parent company auditors or other relevant sources to corroborate or enhance its risk assessment and to ensure that areas of weakness are appropriately considered in its audit plan;
- f) Proactively follows up and reports on significant internal control, risk management and governance issues to ensure timely resolution and escalation to the Board and Senior Management as necessary;
- g) Demonstrates it can cause necessary changes in the operations of the institution in response to material weaknesses identified;
- h) Appropriately considers the pervasiveness and significance of its findings, both at the individual activity level, as well as in aggregate across the institution; and
- i) Appropriately differentiates between audit findings of a prudential nature from those affecting operating efficiency, and the manner in which these are communicated, monitored and followed up.