Workplan for the Internal Audit Function of the System Organization for 2018-2020

This document presents a 3-year rolling internal audit plan for the System Organization (in regard to the operations of the System Management Office) for the period of 2018-2020. The System Organization contracts in-house internal audit resources to provide assurance on System Organization’s governance, risk and controls.

This plan was reviewed and endorsed by the Audit and Risk Committee of the System Management Board.

Issued: Wednesday 28 March 2018
ASSUMPTIONS AND APPROACHES

In arriving at the proposed assurance and advisory engagements, several assumptions were made. These also determined approaches to be used in delivering assurance and advisory work at the System Organization.

- Resources will be available to deliver the plan.
- Based on our prior knowledge we have completed an assurance map for the System Organization. As 2018 will be the first year of the new arrangements delivering audit services for the System Organization, in each of the engagements we will strive to assess both 1st and 2nd lines of defense to validate our assurance mapping and to assess the strength of controls at each level.
METHODOLOGY

• Risks and audit universe under the control and management of the System Organization were assessed (Section I).

• We took note of the past audits and reviews of other assurance providers to avoid duplication (Section II).

• Changes in systems and processes, and the progress of their development at the System Organization affect the timelines of audit engagements.

• Building on the System Organization’s risk management practices, we used internal audit’s own risk assessment, and stakeholders’ feedback to guide the engagement selection and prioritization (Section III).

• Assurance activities at the 3 lines of defense were mapped against the audit universe to help identify areas lacking assurance coverage (Section IV).

• The proposed engagements for the 2018-2020 are laid out in Section V.
SECTION I.
Audit universe of the System Organization

System Management Office

Support CGIAR mission what are we here for
- Council and Board support
  - Support meetings & reporting
  - Governing documents/ToRs
- Funder and external relations
  - Funder relations
  - Contributions
  - Funding agreements
  - Partnerships
- Portfolio support
  - Financial Planning & management of contributions
  - Portfolio reporting: financial/non-financial
  - Performance management system
  - Fund allocation & disbursement

Operations the things we do here
- Financial accounting
- Financial planning & reporting
- Communications
- Procurement
- Admin support
- Facilities management
- Legal
- Protocol
- HR
- Staff safety & security
- IT
- IP support

Culture, control environment three lines of defence
- first line (risk ownership)
  - Governance: strategies and oversight (ARC, ET)
  - Organisational policies, ethical standards, accountability frameworks, tone at the top
  - Risk Management & Business Continuity Management
  - Whistle-blowing, fraud awareness and prevention
- second line (risk oversight)
  - independent assurance: internal audit
- third line (Independent verification)
  - independent assurance: external audit
  - System reporting

Organisational projects:
- OCS implementation
- Review of policy framework
- Ways of working: task teams
- Work planning and budgeting
SECTION II. Previous engagements

Audits delivered in the last 3 years for the System Organization (previously CGIAR Consortium) under the old, broader mandate, of the CGIAR Shared Services Internal Audit Unit

<table>
<thead>
<tr>
<th>2017</th>
<th>2016</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board tool (Advisory)</td>
<td>Interim accounts</td>
<td>CRP Letters of agreement</td>
</tr>
<tr>
<td>Fraud risk assessment (Advisory)</td>
<td>ICARDA investment plan</td>
<td>IT risks and controls</td>
</tr>
<tr>
<td>Payments for ICARDA</td>
<td>CRP audits (Phase I and II)</td>
<td>CRP audits (Phase I)</td>
</tr>
<tr>
<td>OCS application controls</td>
<td>Follow up on audit recommendations</td>
<td></td>
</tr>
<tr>
<td>Human Resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow up on audit recommendations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECTION II. Coverage of the audit universe by previous engagements

Below are the elements of the System Organization audit universe and areas covered by previous reviews.

- 2017 coverage
- 2016 coverage
- 2015 coverage

Fully colored boxes in green, amber and yellow indicate substantial coverage, and the colored frames – partial coverage.
SECTION III. Top risks and concerns

Top concerns of stakeholders and internal audit

1. SMO business model and processes
2. SMO capacity
3. SMO value for money and efficiencies/cost-effectiveness
4. Internal communications
5. SMO risk management
6. Compliance with GDPR
7. Talent management
8. SMO policies and procedures
9. Document retention

The main stakeholder concern is around effectiveness of the organizational arrangements at the System Organization, followed by concerns over its cost-effectiveness.
SECTION IV. Mapping of assurance providers

The table maps out assurance activities implemented in 2016-2017 and planned in 2018. The activities of the 1st and 2nd lines of defense are completed to the best of our knowledge and will be reviewed as part of our engagements and interactions with System Organization’s staff and management.
Each proposed engagement will cover a number of concerns raised, and the 2018 audit plan will aim to address the most pressing needs in assurance. The engagements proposed for 2019 and 2020 will be reviewed again at the end of 2018 vis-à-vis changed risks and concerns to ensure that assurance provided remains relevant.

<table>
<thead>
<tr>
<th>Engagements/ Top concerns</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Data Protection Regulation (GDPR) readiness (2018)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management (2018)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business planning, resourcing and structuring (2018)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>General ICT controls (2019)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opportunities for value for money (2018)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal communications (2019)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Talent management (2019)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OCS follow up (2020)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy framework (2020)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document retention and archiving (2020)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## SECTION V. Proposed engagements by year

<table>
<thead>
<tr>
<th>2018</th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>• General Data Protection Regulation (GDPR) readiness</td>
<td>• General ICT controls</td>
<td>• OCS follow up</td>
</tr>
<tr>
<td>• Risk management</td>
<td>• Business processes: accounting, cash management &amp; procurement</td>
<td>• Policy framework</td>
</tr>
<tr>
<td>• Opportunities for value for money</td>
<td>• Internal communications</td>
<td>• Document retention and archiving</td>
</tr>
<tr>
<td>• Follow up on audit recommendations</td>
<td>• Talent management</td>
<td>• Follow up on audit recommendations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2018</th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>
### Section V. Proposed engagements -2018

<table>
<thead>
<tr>
<th>Risks</th>
<th>Type of engagement</th>
<th>Rationale</th>
<th>Potential objectives and scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR readiness</td>
<td>Advisory</td>
<td>• The updated European law on data protection has deadline for its implementation as May 2018 and includes steep fines for non-compliance &lt;br&gt; • As the System Management Office employs European citizens and processes their data, some elements of the law will need to be complied with.</td>
<td>Throughout the engagement, we will aim to work with management to identify to what extent the law is applicable to the System Management Office, business areas that are affected, and evaluate the plans to ensure compliance.</td>
</tr>
<tr>
<td>Risk management</td>
<td>Advisory</td>
<td>Risk management activities are important to ensure that the office anticipates and responds to external and internal threats proactively to strengthen its position. Internal Audit should be able to rely on a robust risk management system.</td>
<td>Internal audit will work with management to identify key elements of a risk management framework that will help the System Organization to achieve its objectives in a more efficient and effective manner.</td>
</tr>
</tbody>
</table>

*Table:* Proposed engagements -2018
## SECTION V. Proposed engagements -2018

<table>
<thead>
<tr>
<th>Risks</th>
<th>Type of engagement</th>
<th>Rationale</th>
<th>Potential objectives and scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunities for improved value for money</td>
<td>Assurance</td>
<td>The role of the System Organization is changing as its ways of working; new approaches and structures are being tested. There are also expectations that the System Management Office will conduct its business in an efficient and cost effective way delivering value for money to its stakeholders. If it is not the case, System Management Office’s ability to achieve its objectives as well as its reputation will be negatively affected, staff morale will drop resulting in loss of talent.</td>
<td>Efficiency, cost-effectiveness and value for money are rooted in clarity of purpose, good planning and streamlined processes. The review will assess the existence and adequacy of business objective setting and planning as well as will dive-in to specific processes to evaluate to what extent opportunities for delivering value for money (maximizing productivity while using resources efficiently and effectively) are exploited. Potential processes to be evaluated will be specified in the ToR of the engagements and may include but not limited to budgeting and procurement.</td>
</tr>
<tr>
<td>Follow up on internal audit recommendations</td>
<td>Assurance</td>
<td>To provide ARC with overview of the progress of addressing risk and control weaknesses identified by internal audit.</td>
<td>The review will follow up on the implementation of audit recommendations assigned to management at the System Organization and which are due as of end of 2018.</td>
</tr>
</tbody>
</table>
Section V. Coverage of the audit universe by proposed engagements

Areas to be covered by assurance activities of the proposed 2018 audit plan: