| Agency Name: | |  | | | |
| --- | --- | --- | --- | --- | --- |
| Plan Version Number: | |  | Plan Date: | |  |
| Reviewer Name: | |  | Review Date: | |  |
| # | Question | | Y/N | Feedback | |
| 1 | Does the assurance plan provide clear information on the top ICT risks for the agency and their potential impact on business outcomes? | |  |  | |
| 2 | Is the scope of the assurance plan clear?  *It is expected that the assurance plan will cover assurance activities for the next financial year and will be updated on annual basis before the start of each financial year. Note the date the assurance plan will be next reviewed and updated.* | |  |  | |
| 3 | Does the assurance plan describe how lessons learned have been incorporated into the assurance approach?  *For example, lessons learned from prior year activities, other assurance activities or system level lessons learned applicable to the agency and its ICT environment.* | |  |  | |
| 4 | Are decisions, assumptions and trade-offs made in developing the assurance plan clearly stated?  *This may include acceptance of a lower level of assurance due to resourcing constraints, other factors, etc. The assurance plan should describe any gaps in assurance and these will be closed, including a timetable.* | |  |  | |
| 5 | Are estimated assurance costs clearly stated in the assurance plan and have they been budgeted for? | |  |  | |
| 6 | Is there a clear link between top ICT risks and planned assurance activities?  *Top risks include information security; service continuity; service portfolio management, including legacy ICT risk; vendor management; and capacity management, including resource capacity and capability constraints.* | |  |  | |
| 7 | Is the assurance approach integrated across all ‘three lines of defence’?  *The ‘three lines of defence’ model includes day-to-day operational management processes and controls, governance and oversight arrangements for ongoing monitoring of risks as well as independent assurance from internal (e.g. Internal Audit) and third party assurance providers, including External Audit.* | |  |  | |
| 8 | Are assurance activities coordinated?  *Roles and responsibilities across assurance providers should be clearly defined and coordinated to reduce the compliance burden on delivery teams and maximise value for money.* | |  |  | |
| 9 | Are assurance roles and responsibilities clearly defined?  *For example:*   * *Who will be responsible for ensuring that ICT risks are managed and owned at the right level within the agency?* * *Who will be responsible for monitoring and reporting top ICT risks?* * *Who will review and approve the assurance plan and other key assurance artefacts (e.g. terms of reference and reports for independent assurance reviews)?* * *How will progress against the assurance plan be monitored?* * *How will the status of issues raised in assurance reports be tracked and reported at the governance level?* | |  |  | |
| 10 | Has the assurance plan been approved at the appropriate level?  *The assurance plan should be approved by the Chief Executive and/or appropriate ICT governance body. It is expected that Chief Information Officer and Head of Internal Audit will endorse the assurance plan.* | |  |  | |