Audit and Assurance Committee

Date: **13 July 2017**

Item: **External Quality Assessment of Internal Audit**

This paper will be considered in public

1 Summary

1.1 The purpose of this paper is to present to the Committee the report, dated 29 March 2017, from the External Quality Assessment of Internal Audit prepared by the Chartered Institute of Internal Auditors (IIA).

2 Recommendation

2.1 The Committee is asked to note the paper.

3 Background

3.1 TfL commissioned the IIA to carry out an External Quality Assessment of Internal Audit. This is in accordance with Public Sector Internal Audit Standards, which requires public sector internal audit functions to be subject to an external assessment at least every five years. The previous external assessment was carried out in late 2012.

3.2 The findings from the review are set out in the attached report. The report concludes that Internal Audit generally conforms to the IIA's professional standards, with just three out of 56 areas where there is only partially compliance. The report makes recommendations to achieve full compliance and includes some further recommendations to improve the overall effectiveness of the function.

3.3 We have accepted the recommendations that have been made and our responses have been incorporated into the report. The majority of the recommendations will be addressed through the Corporate Assurance Transformation, which is just getting underway and is discussed elsewhere on this agenda.

3.4 We will update the Audit and Assurance Committee on progress with addressing the IIA's recommendations at future meetings.

List of appendices to this report:

Appendix 1 - External Quality Assessment Report on TfL Internal Audit dated 29 March 2017

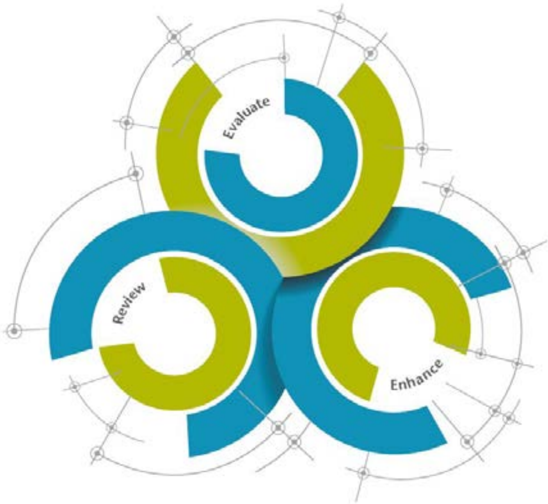
List of Background Papers:

None

Contact Officer:	Clive Walker, Director of Internal Audit
Number:	020 3054 1879
Email:	Clivewalker@tfl.gov.uk

Chartered Institute of Internal Auditors

Appendix 1



EXTERNAL QUALITY ASSESSMENT (EQA) REPORT FOR

Transport for London

Prepared by Chris Butler and Malcolm Zack on behalf of the Chartered Institute of Internal Auditors, 29th March 2017

TABLE OF CONTENTS

The EQA was concluded on 29th March 2017 and provides management and the Audit Committee with information about Internal Audit as of that date. Future changes in environmental factors and actions taken to address recommendations, may have an impact upon the operation of Internal Audit in a manner that this report cannot anticipate. Considerable professional judgment is involved in evaluating. Accordingly, it should be recognized that others could draw different conclusions. This report is provided on the basis that it is for your information only and that it will not be quoted or referred to, in whole or part, without the prior written consent of Chartered IIA.

EXECUTIVE SUMMARY

The review was based on an internal assessment of conformance conducted by TfL internal audit in 2015. Our review confirmed changes and updates since that time by examining audit documentation, reports and files and interviewing a range of audit staff and stakeholders. We have benchmarked the department, as it currently stands, against our knowledge of other audit departments we have reviewed in the previous year. We make recommendations on ways to achieve full conformance to the standards and make observations on how to enhance the value and effectiveness of the department. We were also asked to take account of the emerging proposals to transform the audit department and its relationship with other governance and assurance providers and offer a view on the options and direction of travel.

In our view TfL internal audit generally conforms to the IIA's professional standards with partial conformance in only 3 out of 56 areas. We make three recommendations to achieve full conformance and offer some views on how to improve overall effectiveness.

Current possible organisational changes are being considered and we think the following principles should be carefully considered:

- Make clear to whom each assurance provider report and for what purpose they exist
- Be clear where assurances on financial control, technical compliance, Health and Safety etc are derived from
- Ensure that Internal Audit can form an objective opinion on each second line of defence function
- Ensure that Internal Audit have the necessary skillsets to review the second lines of defence
- Attain the right balance between second and third line, avoiding duplication
- All assurance functions use a common agreed risk assessment so that assurance efforts properly address the most important issues

We would recommend that a more detailed mapping exercise be carried out which demonstrates the linkages and possible overlaps and gaps.

Conformance to the International Professional Practice Framework

The objective of this External Quality Assurance (EQA) review was to undertake an independent assessment of the effectiveness of TfL's internal audit function using as a starting point TfL's own assessment carried out in 2015. This has included considering the team's conformance to the IPPF, benchmarking the function's activities against best practice and considering the possible changes arising from the transformation project currently underway.

The Institute of Internal Audit's (IIA's) International Professional Practice Framework (IPPF) includes the Definition of Internal Auditing, Code of Ethics and *International Standards*. There are 56 fundamental principles to achieve with more than 150 points of recommended practice. Below is a summary of TfL's internal audit function's conformance to the IPPF showing that it generally conforms to all but 3 of the standards. This is a good performance given the breadth of the IPPF and the challenges facing the function.

Summary of IIA Conformance	**Standards**	**Does not Conform**	**Partially Conforms**	**Generally Conforms**	**Not Applicable**	**Total**
Definition of IA and Code of Ethics	Rules of conduct			5		5
Purpose	1000 - 1130			7		7
People	1200 - 1230		2	2		4
Performance	1300 - 1322			6	1	7
Planning	2000 - 2130		1	10	1	12
Process	2200 - 2600			20	1	21
Total			3	50	**3**	**56**

It should be noted that changes to the IPPF came into force in January 2017. The revisions include the addition of two new standards, alignment of the *Standards* to the Core Principles, and updates to existing standards. While this assessment is against the previous standards the observations made take account of the revisions.

The review did not include an evaluation of the working practices of the fraud team. It did include the now integrated Crossrail Audit team and the Health, Safety, Environmental and Technical audits. To understand the context of the transformation programme we also sought to understand the relationship internal audit has with other assurance providers such as strategic risk and project assurance.

During the review we were made aware of the independent review on the audit of the Garden Bridge design and engineering support procurements. We reviewed the report and examined some of the associated audit working papers so as to take account of any issues relevant to our assessment of the department's conformance with IIA standards.

The overall assessment resulting from the EQA is that the internal audit function generally conforms to the IIA's professional standards with only three areas of partial conformance and three standards which were not applicable. This conclusion relates to the internal audit department as currently established. Later we consider challenges which may arise depending upon which organisational options are adopted.

Key Achievements

Internal audit is valued by senior management and their engagement in audits and consulting is often sought

Audit Charter including a mission statement (although not aligned to the IIA's recommended mission for Internal Audit)

Comprehensive and consultative approach to annual planning using workshops with management

Coordination with other assurance providers and production of an annual integrated assurance plan incorporating three year plans

A comprehensive Annual Internal Audit report which goes to the Audit Committee

Internal Audit Strategy produced in 2013 and updated in 2015/6

Integration of Crossrail internal audit into the audit department in spring 2016.

The Transformation Programme

At the time of the review a number of options for organisational change were being considered but no final decisions had been reached. We had discussions with a range of key stakeholders to try and understand the issues and potential pitfalls. We were impressed by the degree of coordination there was already between the various assurance providers and the production of an annual integrated assurance plan. However it seems that despite the best efforts there was still the view that there was confusion between roles and some duplication of effort, particularly in relation to project assurance.

In considering these issues the key principles seem to be:

- to retain sufficient independence and safeguards for Internal Audit so that it can provide fully objective opinions on risk, governance and control including an objective opinion on each second line of defence function
- to make clear to whom each assurance provider reports and for what purpose they exist
- to make clear who is responsible for assurance on financial control, technical compliance, Health and Safety, project funding decisions etc
- ensure that Internal Audit has the necessary skillsets to review the second lines of defence
- attain the right balance of effort between second and third line, avoiding duplication
- ensure that all assurance functions use a common agreed risk assessment so that assurance efforts properly address the most important issues
- arrangements need to be as simple as possible so that it is obvious who is doing what.

Internal audit requirements

IA needs to be able to form a view on the organisation's risk management processes and their effectiveness. If assurance providers are brigaded with internal audit safeguards are needed to ensure that it remains sufficiently independent to provide objective assurance to the board and audit committee. Conversely where there are useful synergies between assurance providers these should be exploited.

The person acting as Chief Audit Executive needs sufficient independence to provide objective assurance free from the risk of being overridden. This can be achieved by giving the CAE a direct reporting line to the Commissioner and the Audit Committee in addition to any administrative line to a head of Risk and Assurance.

Conclusions

We have seen examples of Internal Audit and Risk being merged or with Internal Audit reporting through a Head of Risk or Chief Risk Officer. With the right safeguards to preserve audit independence these arrangements can work.

Recommendations to achieve conformance to the Standards

1210 Proficiency	**Response & action date**
We recommend urgent completion of the development of a competency matrix and an analysis of the skills needs demanded by the audit plans and the identification of any corresponding skills gaps. This will also aid any organisational changes resulting from the transformation programme.	Work is currently underway to build on the draft framework and matrix with the aim of identifying the skills/ knowledge and competencies required to deliver our plans, and to highlight any gaps. This will be an important feed into our transformation programme. The final version will clearly distinguish between levels of staff and align with both the IIA and TfL Competency Frameworks. 30 April 2017
1230 Continuing Professional Development	**Response & action date**
CPE/CPD is a requirement of the IIA standards. While recognising the resource constraints we strongly advise more attention is given to agreeing CPE with staff. This does not need to involve expenditure on training but can be achieved by self-study, internal seminars and stretching work experience. Linked to the previous recommendation, CPE can help close off any skill gaps within the department.	We will continue to promote non-cost and lower cost methods of developing staff professionally. The department's approach will need to be sufficiently flexible to recognise the differing institute requirements for CPE/ CPD. Specifically this will involve: • Completion of the Competency Framework which will incorporate technical competency requirements of the different institutes. • Collation of the alternative training/ learning opportunities within and outside TfL discussed at the recent department meeting.

	• As part of ongoing performance management processes, line managers will have a responsibility to be aware of their staffs' requirements and ensure relevant actions are taken to meet CPD/ CPE requirements. 31 May 2017
2320 Analysis and Evaluation	**Response & action date**
The basis for evaluation of the adequacy of risk mitigation, both in design and in operation, is not always clearly documented showing reasons for conclusions. The audit programme risk/control evaluation schedule should be more explicit in its requirements. Risks should be defined clearly, overall conclusions by risk should be shown (not just by individual control) and where possible the consequences of mitigation failure evaluated. We recommend amendments to the audit manual and to the control evaluation schedule to facilitate this key part of the audit process.	The Processes and Systems element of the Corporate Assurance Transformation workstream will incorporate these recommendations in its review of processes and the Audit Manual. This will include: • Ensuring that key risk areas identified as part of planning are agreed at a sufficiently senior level. • A revision to the audit programme template to ensure that: o Controls are properly described – eg not just the absence of the risk. o Conclusions are made at the key risk area level and not just for each individual control. • The implications of the above for reporting. The above points to be included in the revised Audit Manual and communicated to staff. 30 September 2017

Scope for Further Development

The Chartered Institute regards conformance to the IPPF as the foundation for effective internal audit practice. However, our EQA reviews also seek feedback from key stakeholders and we benchmark each function against the diversity of professional practice seen on our EQA reviews and other interviews with chief audit executives, summarised in an Internal Audit effectiveness matrix. We then interpret our findings into scope for further development based upon the wide range of guidance published by the Chartered Institute. It is our aim to offer advice and a degree of challenge to help internal audit activities continue their journey towards best practice and excellence.

In the following pages we present this advice in three formats.

- An analysis to recognise the accomplishments of the team and to highlight potential threats and opportunities for development.
- A matrix describing the key criteria of effective internal audit, highlighting the level TfL IA has achieved and hence the potential for further development.
- A series of recommendations for further development which internal audit team could use as a basis for an action plan.

For us the main areas for discussion are around:

- Providing more opportunities for rotation of staff
- Updating audit methodology to improve scoping the audit and more focus on evaluation of risks
- More use of audit tools
- Improving management and flexible deployment of resources and use of KPIs

We should stress, however, that, except for the three standards listed above, the internal audit function generally conforms. The existence of opportunities for improvement, better alternatives, or other successful practices does not reduce a generally conforms rating.

SWOT ANALYSIS

What works well (Strengths)	**What could be done better (Weaknesses)**
• Consulting engagements • Staff with good experience of the business and technical skills • Mainly sound methodology • Recognition of the importance of coordinating assurance • Support from Senior management for the role of internal audit	• Better engagement with the client to ensure audits cover the important issues • Reduce the size of some of the reports and papers to the audit committee • Better definition of risks • Evaluation of risk mitigation and the consequences of ineffective mitigation • More sharing of knowledge and experience within the department • Reduce time between closing meeting and issue of "final" interim report. This could be helped by emphasising that management should respond to drafts within a reasonable timescale.

What could deliver further value (Opportunities)	**What could stand in your way (Threats)**
• Tracking function in AutoAudit • Use of data analytic tools • Higher level audits such as Audit of safety Culture • Simplification of the assurance arrangements • Selective outsourcing of audits requiring particular skills • Greater rotation of staff and co-opting staff onto audits where they can bring in particular knowledge and experience. • Use better targeted KPIs to encourage improved efficiency	• Loss of key staff and inability to replace them • Potential for Transformation programme to cause loss of internal audit independence and confusion between the roles of different assurance providers • Need to maintain awareness of the business

Internal Audit Maturity (current position prior to any organisational changes)

Assessment	CIIA standards	Focus on performance, risk and adding value.	Coordination and maximising assurance	Operating with efficiency	Quality Assurance and Improvement Programme
Excellent	Outstanding reflection of the CIIA standards, in terms of logic, flow and spirit. Generally conforms in all areas.	IA alignment to the organisation's objectives, risks and change. IA has a high profile, is listened to and is respected for its assessment, advice and insight.	IA is fully independent and is recognised by all as a 3rd line of defence. The work of assurance providers is coordinated with IA reviewing reliability of other assurance providers.	Assignments are project managed to time and budget using tools/techniques for delivery. IA reports are clear, concise and produced promptly.	Ongoing efforts by IA team to enhance quality through continuous improvement. QA&IP plan is shared with and approved by AC.
Good	The CIIA Standards are fully integrated into the methodology – mainly generally conforms.	Clear links between IA engagement objectives to risks and critical success factors with some acknowledgement of the value added dimension.	Coordination is planned at a high level around key risks. IA has established formal relationships with regular review of reliability.	Audit engagement are controlled and reviewed while in progress. Reporting is refined regularly linking opinions to key risks.	Quality is regarded highly, includes lessons learnt, scorecard measures and customer feedback with results shared with AC
Satisfactory	Most of the CIIA Standards are found in the methodology with scope to increase conformance from partially to generally conform in some areas.	Methodology requires the purpose of IA engagements to be linked to objectives and risks. IA provides advice and is involved in change but criteria and role require clarity.	The 3 lines of defence is model is regarded as important. Planning of coordination is active and IA has developed better working relationships with some review of reliability.	Methodology recognises the need to manage engagement efficiency and timeliness but further consistency is needed. Reports are informative and valued.	Clear evidence of timely QA in assignments with learning points and coaching. Customer feedback is evident. Wider QA&IP may need formalising.
Needs improvement	Gaps in the methodology with a combination of non-conformances and partial conformances to the CIIA Standards.	Some connections to the organisation's objectives and risks but IA engagements are mainly cyclical and prone to change at management request.	The need to coordinate assurance is recognised but progress is slow. Some informal coordination occurs but reviewing reliability may be resisted.	Multiple guides that are slightly out of date and form a consistent and coherent whole. Engagement go beyond deadline and a number are deferred.	QC not consistently embedded across the function. QA is limited / late or does not address root causes.
Poor	No reference to the CIIA Standards with significant levels of non-conformance.	No relationship between IA engagements and the organisation's objectives, risks and performance. Many audits are adhoc.	IA performs its role in an isolated way. There is a feeling of audit overload with confusion about what various auditors do.	Lack of a defined methodology with inconsistent results. Reports are usually late with little perceived value.	No evidence of ownership of quality by the IA team.

Recommendations for Further Development

We offer a range of ideas and recommendations to improve the effectiveness and efficiency of internal audit.

Governance	**Response & action date**
The Audit Charter will need to be updated to bring it in line with latest changes to the IPPF. The Mission should reflect the IIA's formula which is "To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." The Charter should also refer to the core principles which can provide a framework for the Audit Committee and Board to form an opinion on whether IA continues to conform to the IIA Standards. Some Directors would like to see reports from other areas and be kept informed of impending audits. Some stakeholders would like more visibility of audit programme through the year and sight of findings from other parts of the business (at Director level). These ideas should be considered in the context of the audit charter, the implications for client confidentiality and the decision to stop the use of interim/ final audit reports. In addition the Charter should be amended once decisions are taken resulting from the Transformation Programme.	Once Transformation is complete the Charter will be updated to bring it in line with the latest changes to the IPPF, revise the mission as required, refer to the core principles and incorporate outcomes from the Transformation Programme itself. One of the proposals being taken forward through the Corporate Assurance Transformation workstream is for Internal Audit to take proactive measures to promote corporate knowledge. This will include agreement of an approach to sharing of information about the audit programme and completed audits. 30 September 2017
People	**Response & action date**
We would recommend more use of secondments into and out of internal audit. IA should be viewed as a valuable place to work to gain experience of TfL and secondees can also bring a fresh perspective to the audit department.	We will explore with the business options for incorporating a programme of inward and outward secondments into Internal Audit as part of the resourcing strategy for the department post Transformation. 30 September 2017
Methodology	**Response & action date**
Ensure that risks being assessed in the audit are well defined and recorded in	Response and action date same as for 2320 above.

the work programme alongside the anticipated controls. This will help the audit team ensure they have addressed each risk being assessed before arriving at an overall conclusion on the area being reviewed. There should be greater engagement with the auditee and sometimes this should be at a more senior level so as to ensure the audit really addresses the key issues and that management buy-into the audit. This should start with the development of the letter of engagement to ensure the audit is properly scoped from the outset. It may be that more involvement is needed by audit managers and senior audit managers to ensure this works and to ensure that auditors are properly briefed on the reason for the audit (the Audit Objective) and understand enough about the business area.	
Tools and Techniques	**Response & action date**
AutoAudit works well as a documentation tool. It has a tracker function which is not being fully used to keep track of audit recommendations. IDEA is not much used apart from in the fraud team. Given the data rich nature of TfL it would seem more use could be made of analytic and reporting tools. The use of email search facilities should also be considered.	The Internal Audit Leadership Team took the decision to discontinue the AutoAudit tracker function Issue Track due to ongoing system problems which could not be resolved by Thomson Reuters. Issue Track will therefore no longer be used. Action progress is tracked in AutoAudit by audit management and reported weekly on the Audit Actions SharePoint site and periodically to senior management. The analytics specialists are increasingly being used to support audit work as well as fraud investigations, and this trend will continue. More generally the department’s future approach to the use of analytical and reporting tools will be defined through the Transformation Programme. We also plan to use the SAP Governance, Risk and Control tool being developed by the Financial Shared Services Centre to monitor and analyse the operation of financial controls. 30 May 2017

Quality	**Response & action date**
The current Quality Assurance and Improvement Programme needs to be reviewed on the back of this review and the transformation project. An internal assessment should also be conducted in 2017/18 after changes from this review and transformation. The audit committee should be kept informed of progress on the QAIP.	Our annual Quality Assurance and Improvement Programme will include a review of changes following this EQA and the Transformation Programme. The outcomes of this will be reported to the Audit and Assurance Committee, as it is currently. 31 March 2018
Managing performance	**Response & action date**
It is not clear to us how overall resources are managed and redeployed as vacancies appear and audit plans are revised. It is also not clear what process is used to get agreement to cancellations or postponements. There has been some feedback that audit are not as responsive as they could be to new or urgent demands. Quarter 1 and 4 progress reports show changes to the plan but not an explanation for them. AutoAudit resources budget tab is not used. Audits are controlled by timescale rather than man-day budgets. KPIs need to be more relevant to actual performance. We recommend that the department review their current ways of managing and reporting on use of resources and produce a revised dashboard for their own use and for reporting to the audit committee.	The review of Processes and Systems that forms part of the Corporate Assurance Transformation workstream will incorporate these recommendations. We are currently changing the audit planning process to make the audit plan more flexible especially at a time of such organisational change. This will ensure that changes to the plan are tracked and reported including documenting agreement to cancellations and postponements. The report to the Audit and Assurance Committee has been revised to include explanations for changes to the plan. The Internal Audit Leadership Team decided in 2016/17 to improve the delivery of audits by focusing on milestones rather than budgets. The effectiveness of this is currently being reviewed and will be changed if necessary. A review of the Internal Audit KPIs will be undertaken to consider both the IIA recommendations and the new General Counsel Scorecard. We will also consult with the Audit and Assurance Committee over the KPIs it wishes to

	see. 30 September 2017
Probity	
There should be a process for identifying and documenting impairments to objectivity. Similarly it would be prudent to remind staff periodically of the need to register and offers of gifts and hospitality.	The acceptance of gifts and hospitality process is noted in the Audit Manual at 10.3 but does not make reference to other potential impairments to objectivity. A process for identifying and documenting impairments to objectivity will be incorporated into the Audit Manual. Reminders will be sent to staff periodically. 30 September 2017

IIA GRADING DEFINITIONS **Appendix 1**

The following rating scale has been used in this report.

Overall Audit Grading	
Generally Conforms (GC)	The assessor has concluded that the relevant structures, policies, and procedures of the activity, as well as the processes by which they are applied, comply with the requirements of the individual Standard or element of the Code of Ethics in all material respects. For the sections and major categories, this means that there is general conformance to a majority of the individual Standards or elements of the Code of Ethics, and at least partial conformance to the others, within the section/category. There may be significant opportunities for improvement, but these must not represent situations where the activity has not implemented the Standards or the Code of Ethics, has not applied them effectively, or has not achieved their stated objectives. As indicated above, general conformance does not require complete/perfect conformance, the ideal situation, successful practice, etc.
Partially Conforms (PC)	The assessor has concluded that the activity is making good-faith efforts to comply with the requirements of the individual Standard or element of the Code of Ethics, section, or major category, but falls short of achieving some major objectives. These will usually represent significant opportunities for improvement in effectively applying the Standards or Code of Ethics and/or achieving their objectives. Some deficiencies may be beyond the control of the activity and may result in recommendations to senior management or the board of the organisation.
Does Not Conform (DNC)	The assessor has concluded that the activity is not aware of, is not making good-faith efforts to comply with, or is failing to achieve many/all of the objectives of the individual Standard or element of the Code of Ethics, section, or major category. These deficiencies will usually have a significant negative impact on the activity's effectiveness and its potential to add value to the organisation. They may also represent significant opportunities for improvement, including actions by senior management or the board.

Often, the most difficult evaluation is the distinction between general and partial. It is a judgement call keeping in mind the definition of general conformance above. The assessor must determine if basic conformance exists. The existence of opportunities for improvement, better alternatives, or other successful practices does not reduce a “generally conforms” rating.

Appendix 2

List of Interviewees

Name	Title/Position	Contact type
Ian Nunn	Chief Finance Officer	Interview
Graeme Craig	Director of Commercial Development	Interview
Nick Fairholme	Director of Projects and Programmes	Phone
Sarah Bradley	Group Financial Controller	Interview
Howard Carter	General Counsel	Interview
Richard Bevins	Head of Information Governance	Interview
Tricia Wright	Human Resources Director	Interview
Anne McMeel	Chair of TfL Audit and Assurance Committee	Interview
Robert Jennings	Chair of Crossrail Audit Committee	Phone
Jill Collis	Director of Health, Safety and Environment	Interview
Karl Havers	External Audit (EY)	Phone
Andrea Cutinha	Group Strategic Risk Manager	Interview
Michael Bridgeland	Head of Project Assurance	Interview
Clive Walker	Director of Internal Audit	Interview
Colin Garland	Senior Audit Manager Business Processes	Interview
Roy Millard	Senior Audit Manager Commercial and Business Support	Interview
Robert Kemp	Senior Audit Manager HSE&T and Crossrail	Interview
Dili Origbo	Senior Audit Manager IM and Security	Interview

Appendix 3

Thoughts on the Transformation Programme

1. We do not see any problem with the fraud function continuing to be part of the audit family and we believe there are useful synergies.
2. The current Strategic risk function has the role of developing and promoting risk management, challenging the identification and assessment of risk and reporting on risk to the board. This will work better with good collaboration with and support from IA.
3. Many organisations merge aspects of risk management with internal audit. The CIIA believes that in doing so it must be clear that management still owns the management of **risks**, the setting of risk appetite, taking decisions on risk responses and being accountable for risk management. However, because of its understanding of risk and risk management techniques internal audit is often well placed to take a lead in promoting the development and use of risk management, suggesting the use of tools and techniques, gathering information about how risk management is operating and reporting that to management. Depending on how deep the involvement is and how proactive internal audit has been in say developing the risk management strategy it may be that in order to provide a fully objective opinion on risk management internal audit would need periodically to buy in an independent review of the effectiveness of risk management.
4. We believe the proposal to move the strategic risk function to the General Counsel offers the potential for a closer and more productive relationship with internal audit. It could fit within the internal audit department, with the safeguards referred to above, or perhaps preferably it could fit into a governance and project assurance department reporting to General Counsel, possibly linked to the Secretariat team. This would have the benefit that reporting on risk becomes part of the natural agenda of the various committees and the Board.
5. There should be a new drive to get Control Risk Self Assurance embedded in the management culture. Internal audit, working with strategic risk, could facilitate this.
6. What is second line and what is third line can sometimes be in the eye of the beholder, complicated by the fact that TfL has a number of different levels through the operating businesses and their associated contractors. Thus a contractor may have both first and second lines of defence assurance functions. Project assurance from TfL then becomes more like a third line and arguably could be confused with internal audit's role. Internal audit should take a view of the coverage, scope and effectiveness of project assurance and the level of risk associated with the projects when forming its audit programme. It could be that certain types of risk are not in scope in the project assurance reviews leaving a gap which internal audit should consider filling.
7. Project Assurance refer to themselves as second line assurance, with projects having first line assurance undertaken at a local level to give confidence to the Project/Programme Team, the Programme Board, and the Directors. Project assurance seems to be primarily concerned with business and financial issues important for approving funding. As such they report their findings both to the project and MD of Finance. If they see a

particular issue with a project they will do a Targeted Assurance Review (TAR) which has similarities with an internal audit although the motivation is to support decision making. It would seem that internal audit should be aware of any TARs and the reasons for them and that information should be shared. IA should avoid doing a project audit which duplicates a TAR.

8. Project Assurance does not cover technical issues which might be covered by the Technical Audits conducted by the HSE and T team in internal audit. Therefore there does not seem to be an overlap in this area.
9. Project Assurance also conduct Integrated Assurance Reviews (IAR). The IAR will not provide technical assurance (this role is taken by the business unit's own processes), but will assess the suitability of the design for the purposes of fulfilling the project requirement, as well as carrying out an outline engineering assessment. One of the standard lines of enquiry is Engineering and Technical but it would seem that this covers only high level questions.
10. We have not considered the IIPAG's work or remit as this is a totally independent function.
11. We think that where practical it is better to keep second and third lines of defence clearly separate and distinct. We see the various inspections carried out by Health and Safety Auditors as second line of defence with regulators or ISO certifiers acting as third line. Brigading some of these functions with audit does not so far seem to have caused a problem except that is does not allow for an objective view on the effectiveness of these second line of defence functions. Internal audit may therefore need to buy in an independent review periodically if a sufficiently objective audit cannot be done. Again a safeguard would be to have a designated CAE with a direct reporting line to the Board/AC separate from anyone with a responsibility both for audit and assurance.
12. The PCIDSS work conducted by the IM audit team is second line and does not need to be performed by them although it does need to be performed by an independent function. It is therefore understandable that it is in internal audit. If it is retained recognition needs to be given of the workload involved.
13. Development of an Assurance map would help defining what assurances come from where and where there are gaps and overlaps. It would also allow for a more critical view of the amount of time/resource spent by the various assurance providers and the level in the organisation at which they operate.

Appendix 4

Options for provisioning internal audit

It is often difficult for an internal audit to have expertise in the wide range of subject areas that are needed. For this reason it is common to buy-in at least 5-10% of the audit resource required. This also allows a wider perspective to be drawn on and provides a fresh pair of eyes for selected audits. However there can be disadvantages. The table below shows a range of options with some of the potential advantages and disadvantages of each. It does not consider the cost implications in detail nor, for example, the optimum amount of co-sourcing given the size and needs of the unit. This would need further analysis. Hybrid versions are possible and may be more desirable than any one option.

Option	Advantages	Disadvantages
Existing in-house service (with some buying in of audits)	Knowledge of the business No setup costs Tried and tested No additional management overhead	May have skill gaps Staleness in approach Over-familiarity with systems and organisation
Buy-in the complete service from an outside firm.	Will allow for changes to be made to the service if required. Draws on experience of the firm. May offer higher powered assistance when required.	Needs to be specified and set up Needs contract management May be difficult to get an overall assurance without costing a lot. Audits may be rather superficial. Loss of flexibility and access to audit when you want it.

Keep an in-house Head of Internal Audit and buy in most of the rest	Benefit of continuity and retention of some knowledge of the business	Needs contract management May not be flexible enough to cover for absence of HIA
Keep some or all of staff but have audit managed by an outside partner acting as HIA	Benefit of some continuity and retention of some knowledge of the business. Would allow for refreshing the approach and wider perspective.	Needs contract management Initial loss of knowledge strategically to lead the audit department.
Develop capability of in-house service so as to reduce need for additional bought in services	Benefit of continuity and retention of some knowledge of the business	May not be feasible without high cost of training and development.
Set up partnering arrangement with existing audit unit that has complimentary and relevant skillsets.	Wider perspective and breadth of resource to call upon. Retains concept of having your own dedicated service.	Could be concern about confidentiality of audit information and results and some loss of control of the service. Difficult to find a suitable partner.