INTERNAL AUDIT

Final Assurance Report 2016/17

Risk Management

25th November 2016

Overall IA Assurance Opinion:

REASONABLE

Recommendation Overview:

High Risk	0
Medium Risk	5
Low Risk	3
Notable Practice	0

Review Sponsor:

Jay Patel	Head of Finance & Performance

Report Distribution:

Barry Lister	Senior Assistant Director
Emma Beal	Managing Director

Ownership of all final Internal Audit assurance reports rests with the relevant Review Sponsor.

1. Introduction

1.1 This risk based IA assurance review forms part of the 2016/17 IA Plan. The purpose of this review is to provide assurance to the West London Waste Authority (WLWA) Officers Team and the Audit Committee over the key risks in relation to Risk Management.

2. Background

2.1 Risk management is the process by which risks are identified and evaluated so that appropriate measures can be applied to reduce the likelihood and impact of risks materialising. In the event a risk materialises, this could inhibit the Authority from achieving its objectives and fulfilling its strategic priorities.

2.2 For the Authority, risks are considered as anything that will or has the potential to adversely affect the achievement of service improvement priorities and/or disrupt day to day service delivery. Good risk management aims to achieve compliance with the standards required for good corporate governance.

2.3 Risks can never be entirely eliminated, but proportionate and targeted action can be taken to reduce risks to a level which is deemed acceptable by the Authority. The aim of managing risks is not simply to avoid all risk, but rather to understand the nature of risks and determine the extent to which the Authority can accept risk in seeking to achieve its objectives and strategic priorities.

2.4 Throughout this report we refer to risk management terminology and for ease of reading we have provided a brief definition of some of these terms below:

- **Control** - any action taken by management, the board and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.
- **Risk** - the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.
- **Risk Management** - the process whereby organisations methodically address the risk attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities.
- **Risk Appetite** - The level of risk that is acceptable to the board or management. This may be set in relation to the organisation as a whole, for different groups of risks or at an individual risk level. It provides the benchmark against which WLWA's risk profile is reported, monitored and managed within its risk governance structure.
- **Inherent risk** - the risk that an activity would pose if no controls or other mitigating factors were in place.
- **Residual risk** - the amount of risk left over after natural or inherent risks have been reduced by controls. The general formula to calculate this is Residual Risk = Inherent Risk - impact of control.

3. Executive Summary

3.1 Overall, the IA opinion is that we are able to give **REASONABLE** assurance over the key risks to the achievement of objectives for Risk Management. Definitions of the IA assurance levels and IA risk ratings are included at **Appendix D**. An assessment for each area of the scope is highlighted below:

Scope Area	IA Assessment of WLWA
Policies and procedures	**Reasonable Assurance** **-** The Authority's Financial Regulations (FRs) document the responsibilities of Officers and Members, in particular the Audit Committee, in relation to Risk Management.

Scope Area	IA Assessment of WLWA
	This is underpinned by the Risk Management Framework and Policy which was recently approved by the Audit Committee in September 2016. However, we believe that, in order to further embed a culture of risk management within the organisation this document could be communicated to all staff. Furthermore, a documented and defined risk appetite and a risk tolerance statement could be included clearly stating the risk appetite of the authority. We are pleased to report that the role of the Audit Committee in relation to risk management was found to be adequately captured within their documented Terms of Reference.
Roles and responsibilities	**Substantial Assurance -** It was confirmed through review of the Authorities Financial Regulations, that roles and responsibilities in regards to risk management are clearly defined. Further, risk owners are also clearly stated and included within the risk register, providing further accountability in regards to the ownership of the agreed mitigating action.
Risk identification, classification and evaluation	**Limited Assurance -** We found sufficient controls were in place allowing the Authority to identify, classify and evaluate risks, underpinned by the Risk Management Framework and Policy. This includes a risk classification key ensuring that a standardised approach to risk evaluation is undertaken. We are pleased to report the risks are RAG (Red, Amber and Green) rated, which is seen as good practice as well as being aligned to the PESTEL framework. However, the movement of risks could be further enhanced through the utilisation of a direction of travel indicator to focus resource on deteriorating / materialising risks. The Authority's Officer meeting was found to be an effective forum for corporate risk discussions, allowing for the identification of emerging corporate risks as well as the re-assessment of risks previously captured. However, it is our opinion that further improvements to the risk identification process could be obtained through the implementation of risk based discussions at operational management meetings. This, when coupled with individual service risk registers and appropriate escalation procedures, would prove significant to the early identification and management of risks to service objectives.
Management of risks	**Limited Assurance -** We found significant control weaknesses in the management of the Authority's identified risk. Analysis of the Authority's corporate risk register identified one instance where the inherent risk score was amended throughout the year. Furthermore, instances were identified where the inherent risk scoring was equal to their residual risk scoring, potentially highlighting the insufficient mitigating action undertaken by management to address the risk. Our review highlighted that management action recorded within the risk register was not consistently provided with timescales for action, potentially weakening accountability for mitigating action to be taken.

Scope Area	IA Assessment of WLWA
Monitoring and reporting	**Substantial Assurance -** We were pleased to confirm that the risk register is presented bi-annually to the Audit Committee. This allows the Audit Committee to fulfil its duty and review the risk register and the risk management strategy as per the Authority's FRs. Although we found no standardised report for risks with an unacceptable risk rating; risks were found to be discussed in depth at the Officers monthly meetings.

3.2 The detailed findings and conclusions of our testing which underpin the above IA opinion have been discussed at the exit meeting and are set out in section four of this report. The key IA recommendations raised in respect of the risk and control issues identified are set out in the Management Action Plan included at **Appendix A**. Good practice suggestions and notable practices are set out in **Appendix B** of the report.

4. Detailed Findings and Conclusions

4.1 Policies and procedures

4.1.1 The Authority has Financial Regulations (FRs) in place, which were last approved by the Authority in December 2015. The FR is binding on all employees and provides detailed instructions to assist officers with delegated authority to carry out their duties in a proper manner. Further, they provide the overarching responsibilities within which the Authority manages its risks. The FRs are communicated to all staff members via the Authority's intranet and we are pleased to report that stringent controls are detailed under sections 42 to 44 which, if fully adhered to, will help to mitigate key risks. For example, this details that it is essential that robust integrated systems are developed and maintained for identifying and evaluating all significant strategic and operational risks to the Authority.

4.1.2 The Authority has a Risk Management Policy, Strategy and Framework which underpins the requirements within the FRs. The Risk Management Framework supports the Risk Management Policy and helps improve and strengthen governance and front-line service delivery throughout the Authority. The Policy, Strategy and Framework was reported to the Authority's Audit Committee for approval at their meeting on the 23rd September 2016.

4.1.3 A key requirement of this document, in line with good corporate governance, a risk register is maintained setting out the main risks to which the Authority is exposed and the actions management is taking to mitigate those risks. We confirmed that the review process for the risk register and the risk management strategy are detailed, and this process is reliant on bi-annual Audit Committee review.

4.1.4 However, upon examination of the Authority's intranet site we were unable to locate the updated or the previous Risk Management Policy, Strategy and Framework. Discussion with the Head of Finance and Performance established that this was due to the revised Risk Management Framework and Policy being in the process of being presented to Audit Committee for approval. Nevertheless, it is important that this document is appropriately communicated and made available to all staff to ensure a consistent approach to risk is taken across the Authority. Subsequently, we have raised a recommendation aimed at addressing this risk (refer to **Recommendation 6** in the Management Action Plan at **Appendix A**).

4.1.5 From our review of the Authority's draft Risk Management Policy and Framework it is clear that the Authority is fully committed to effective and efficient RM systems; establishing a framework to identify, assess, treat, monitor and report operational, legal and compliance risks, both those inherent to the nature of the business and those specific to their strategic ambitions.

4.1.6 We undertook an exercise in which we benchmarked the Authority's Risk Management Policy against the International Organisation of Standardisations risk management principles and guidelines, ISO 31000 requirements, as listed in a document published by the Institute of Risk Management (IRM), a structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. We found the Authority to be compliant in 10 out of 13 areas. We found the policy to be partially or non-compliant in three areas. Further detail on these areas of partial or non-compliance can be found in **Appendix C**.

4.1.7 Although the Policy discusses ensuring risks are at an acceptable level, we did not find the Authority's risk appetite to be clearly defined, whilst there is also no risk tolerance statement present. This coupled with the absence of the ISO 31000 requirements (listed above), could in turn diminish the effectiveness of the risk management process due to a lack of a shared understanding of the Authority's view on the level of risk that can and cannot be taken, as well as the mechanisms for assessing risk. Subsequently, we have raised a recommendation (refer to **Recommendation 1** in the Management Action Plan at **Appendix A**).

4.2 Roles and responsibilities

4.2.1 We found the FRs clearly define the roles and responsibilities of Officers and Members in relation to risk management, stating that the Audit Committee is responsible for reviewing the risk register and reviewing the effectiveness of risk management strategy, with the Treasurer responsible for the preparing the Authority’s Risk Management Policy and procedures and for promoting these throughout the Authority.

4.2.2 The FRs are supported by the Risk Management Framework which reiterates these responsibilities as well as stating that Members and the Senior Management Team own, lead and support risk management. We confirmed that the responsibilities of the Audit Committee in relation to risk management are captured within their Terms of Reference.

4.2.3 We are pleased to state that roles and responsibilities can be seen in key mechanisms of the Authority's Risk Management approach. The risk register details a responsible officer against each risk identified acting as the risk owner. We confirmed that risk owners take responsibility for updating the register and highlighting significant changes and new risks. They provide accountability within the Authority's risk management approach, which help to ensure risks are monitored and action is taken.

4.3 Risk identification, classification and evaluation

4.3.1 The Authority's monthly officer meeting provides a forum to facilitate a risk based discussion amongst officer. This mechanism, under the standing agenda item of 'Corporate Governance', provides an opportunity for emerging risks to be discussed and added to the risk register, as well as enabling for updates to be provided on previously identified risks. We are pleased to report that for the three months sampled (May, June and July) evidence was available to support the monthly discussion and update of the risk register.

4.3.2 It is our opinion that the primary focus of the Authority's risk management activity is based on corporate risks with limited focus on operational risks arising. Therefore, we were unable to confirm that operational risk management is embedded throughout the Authority due to the absence of operational risk registers, with no evidence to support risk management discussions within operational management meetings. It is our opinion that this could prove to be a useful source for the identification of emerging risks as well as enhancing the likelihood of achieving operational service objectives. As a result we have raised a recommendation aimed at mitigating the associated risks (refer to **Recommendation 2** in the Management Action Plan at **Appendix A**).

Classification and Evaluation

4.3.3 We are pleased to report that the Authority utilise a standardised approach to the classification and evaluation of risks providing a score, calculated based on an assessment of the impact and likelihood before (inherent) and after (residual) management action to treat the risk. Both the inherent and residual risk rating are provided and a RAG (Red, amber and green) rating. The inherent risk rating is assessed against the mitigating actions detailed in the 'management actions implemented or planned' column of the risk register. From this the residual risk rating is then provided.

4.3.4 The risk ratings are linked to the prioritisation of risks table which is appended to the risk register. Within, the risks with an impact multiplied by likelihood scoring of 20-25 are labelled as red and are seen as requiring immediate management and monitoring. Risks with a score of 9-19 are labelled amber and are seen as requiring management and monitoring, but are less time critical. Finally the risks with a rating of 1-8 are labelled green and are risks requiring ongoing monitoring. It is our opinion that the prioritisation of risk table helps to ensure it is understood across the organisation when mitigating action is required.

4.3.5 Analysis of the Authority's risk register identified that the direction of travel of risks is not classified, enabling management to identify risks that have deteriorated / materialised, require further attention and focus resources. This would also enable management to identify and assess those risks which are improving and potentially implement the same risk management techniques to other risks identified, where applicable. Without providing a summary of direction of travel there is a risk that deteriorating risks will materialises as they are not clearly identifiable within the risk register. As a result we have raised a recommendation aimed at mitigating the associated risk (refer to **Recommendation 7** in the Management Action Plan at **Appendix A**).

4.4 Management of risks

4.4.1 The risk register incorporates a column entitled 'Management Actions implemented or planned' capturing the Authority's approach to managing and mitigating identified risks to the desired level. However, upon review we found that management action taken appeared ambiguous due to a lack of detail as to what action had been taken to date, what further management action required and timelines for this. Without clarity of further management action required, including timeframes, there is an increased likelihood of the risk materialising. As a result we have raised a recommendation aimed at mitigating the associated risk (refer to **Recommendation 3** in the Management Action Plan at **Appendix A**).

4.4.2 Upon analysis of the latest risk register, presented to Audit Committee on 23rd September 2016, we noted risks that had the same inherent and residual risk score (For example risk L3 and L4). This therefore implies that management action taken to date has been insufficient to mitigate the risk or alternatively management have chosen to tolerate this risk. Therefore there is an increased likelihood that this risk will materialise and therefore we have raised a recommendation aimed at mitigating the associated risk (refer to **Recommendation 4** in the Management Action Plan at **Appendix A**).

4.4.3 We selected a sample of two risks (P3c and L3) from the September risk register that had a red or amber RAG rating. In both cases we were able to evidence that management action was updated and mitigating actions had been considered. For example, prior to the addition to the risk register of risk L3 in June 2016, an assessment of the risk had been provided in the general contract update presented at the February 2016 WLWA Officers meeting. However, we found that no standardised risk report is produced when a risk's score and RAG rating reaches Amber or Red. As a result we have raised a recommendation aimed at mitigating the associated risk (refer to **Recommendation 8** in the Management Action Plan at **Appendix A**).

4.4.5 We undertook a further analysis of risk P3c, noting that the inherent score had been altered throughout the year. This implies that the risk had initially been inaccurately assessed; this initial assessment allows the Authority to understand how much resource should be focussed on the identified risk. If the initial assessment is incorrect there is a risk that the controls and mitigating actions put in place will not be appropriate in preventing the risk from materialising. As a result, we have raised a recommendation aimed at mitigating the associated risk (refer to **Recommendation 5** in the Management Action Plan at **Appendix A**).

4.5 Monitoring and reporting

4.5.1 We are pleased to report that Audit Committee receives risk register updates at each of their bi-annual meetings, allowing the Audit Committee to fulfil its duty to review the risk register and the Risk Management Strategy and Framework. As the Audit Committee meets every 6 months, we selected the previous 3 meetings (January 2015, September 2015 and January 2016) for testing and are pleased to report that the risk register was an agenda item, with evidence within meeting minutes to support appropriate discussion on this item.

4.5.2 Furthermore, accountability to stakeholders was fully demonstrated through the above periodic progress reports. In addition, this is provided through assurance statements from the Authority’s Chief Officers and Senior Managers which forms part of the overall governance framework and support the approval of the annual Statement of Accounts. These statements were confirmed to include a section on risk and were reported to the September Audit Committee alongside the Annual Accounts for 2015/16.

4.5.3 It is our opinion that this six monthly reporting, in addition to the monthly officer meeting discussed under para 4.3.1 provides for sufficient reporting and monitoring of corporate risks within the Authority. However, as stated under 4.3.2, we believe there to be further management action required on embedding risk management into day to day operations.

5. Acknowledgement

5.1 Internal Audit would like to formally thank all of the officers contacted during the course of this review for their co-operation and assistance. In particular, the Finance team, whose advice and help were gratefully appreciated.

6. Internal Audit Contact Details

This audit was led by:	Matteo Biondi, CIA **Senior Internal Auditor**
This audit was reviewed by:	Martyn White, CIA **Senior Internal Audit Manager**

Thank you,

Muir Laurie FCCA, CMIIA
Head of Business Assurance

APPENDIX A

Management Action Plan

No.	Recommendation	Risk	Risk Rating	Risk Response	Management Action to Mitigate Risk	Risk Owner & Implementation date
1	The Authority should consider reviewing its Risk Management Policy against ISO31000 - Risk Management. This should include the production of a Risk Appetite Statement to capture the amount and type of risk that it is willing to accept in order to achieve its Strategic objectives (para. ref 4.1.7). We have provided detail of our gap analysis between ISO3001 and the Authority's Risk Management Policy at **Appendix C**.	*If the Authority's Risk Management Policy is not aligned to good practice, then an ineffective approach to Risk Management could be pursued, this in turn could lead to risks materialising.* *If the Authority's risk appetite is not clearly defined, management may have differing interpretations of what is considered an acceptable level in regards to residual risk potentially decreasing the likelihood of achievement of its operational and strategic objectives due to risks materialising or not being managed within acceptable tolerance.*	**MEDIUM** ●	**TREAT**	The risk management policy will be reviewed to define the risk appetite. The policy's next annual review will be at the September Audit Committee.	*Head of Finance* & Performance *(Jay Patel)* *30th September 2017*

Please refer to* ***Appendix D* *for Risk Response definitions.*

Management Action Plan

No.	Recommendation	Risk	Risk Rating	Risk Response	Management Action to Mitigate Risk	Risk Owner & Implementation date
2	Management should consider splitting out the current risk register to ensure it is focussed on the key risks facing the Authority. Consideration should be taken to embed operational risk management within services with associated escalation processes allowing the Authority to identify emerging risks that may crystallise (para.ref 4.3.2).	*If operational risk management is not embedded and escalated throughout the Authority there is an increased likelihood that emerging risks may not be identified and therefore mitigating action cannot be taken. This could lead to a direct financial and reputational loss to the Authority if risks materialise.*	MEDIUM ●	**TOLERATE**	The level of risk management is appropriate to the size and scale of the organisation. Significant risks are reviewed and monitored on a frequent basis by Chief Officers and Senior Management and at every Audit Committee. Operational risks are those which are considered to have very limited impact on the Authority and therefore are managed as part of the operational procedures– e.g. the procurement procedure requires an appropriate evaluation of credit risk, operating vehicles at Twyford requires the daily check for mechanical risks. To collate and maintain registers of all operational risks would be inefficient and in management’s judgement add little value to risk management within the Authority.	*N/A*

Please refer to **Appendix D for Risk Response definitions.*

Management Action Plan

No.	Recommendation	Risk	Risk Rating	Risk Response	Management Action to Mitigate Risk	Risk Owner & Implementation date
3	The Authority should consider separating out management action taken to date and further management action required to manage the risks within the risk appetite / acceptable tolerance. Any further action required should be time bound to help ensure appropriate traction is gained on implementation and risk management (para.ref 4.4.1)	*If mitigating actions are not given an implementation date, there is a risk that the action will be delayed or left incomplete. This then could lead to the risk materialising, leading to a possible financial loss or reputational damage to the Authority.*	**MEDIUM** ●	**TREAT**	The risk register will be updated to include clear actions with clear dates.	*Head of Finance* & Performance *(Jay Patel)* *28th February 2017*
4	Management should ensure that action taken against identified risk reduces the impact and likelihood of the risk materialising. Therefore, unless management chose to tolerate the risk, the residual risk score should be lower than the inherent risk score detailed (para.ref 4.4.2)	*If the residual risk rating is not lower than the inherent risk rating, the mitigating action taken or proposed has failed to reduce the impact and likelihood of the risk materialising. Subsequently, this could lead to a direct financial loss to the Authority or reputational damage.*	**MEDIUM** ●	**TREAT**	The risk register will be reviewed to ensure scoring is appropriate and mitigating actions have an impact on the risk score	*Head of Finance* *(Jay Patel)* *28th February 2017*

Please refer to **Appendix D for Risk Response definitions.*

APPENDIX A (cont'd)

Management Action Plan

No.	Recommendation	Risk	Risk Rating	Risk Response	Management Action to Mitigate Risk	Risk Owner & Implementation date
5	Management should ensure during the initial risk assessment, the likelihood and impact of the risk are considered thoroughly and an accurate inherent risk scoring is provided (para. ref 4.4.5).	*If the inherent risk scoring is altered this may impact upon the effectiveness of original risk treatment options proposed, thus increasing the likelihood that risks materialise and / or are not managed in accordance with the Authority's risk appetite.*	MEDIUM ●	**TREAT**	Risks are included in the risk register as soon as they are identified. Almost all risks will retain their original risk score based on the initial evaluation. However, proper evaluation of some risks may require further information / advice (e.g. legal) to properly score, therefore it may be necessary to update the original score. The proper score needs to be reported so will be included in the register. To provide transparency of the improved evaluation, the old score will also be provided and clearly marked.	*Head of Finance* *(Jay Patel)* *28th February 2017*

Please refer to **Appendix D for Risk Response definitions.*

APPENDIX B

Good Practice Suggestions & Notable Practices Identified

No.	Observation/ Suggestion	Rationale	Risk Rating
6	The Authority should ensure that the Risk Management Policy and Framework are available to all staff, communicated via the intranet and other effective means to help raise the profile, embed a risk based culture and ensure a standardised approach to risk management is implemented throughout the organisation (para. ref 4.1.4).	*If staff do not have access to the Authority's risk management strategy there is an increased likelihood that the Authorities standardised approach to risk management is not adhered to and risk is not captured, managed or escalated in accordance with established processes.*	**LOW** ●
7	Management should consider implementing a direction of travel indicator within the risk register. This will allow for the easy identification of materialising / deteriorating and improving risks thus showing the effectiveness of risk management. Management should also consider presenting a one page summary of the corporate risk register to Audit Committee showing the risk, its rating and direction of travel to ensure Senior Management discussion is focused (para. ref 4.3.5)	*Without the direction of travel shown, management cannot identify risks that are deteriorating and require further attention, whilst emerging risks are also not easily identifiable. Therefore, appropriate mitigating action may not be undertaken which in turn could lead to a financial loss or reputational damage to the Authority.*	**LOW** ●
8	Management should consider introducing a standardised risk report for risks with an Amber or Red residual risk scoring, listing the possible mitigating actions and implementation dates (para. ref 4.4.4).	*In the absence of a standardised risk report when risks reach an unacceptable level, then an uncoordinated approach to risk may be taken across the organisation and mitigating actions may remain incomplete.* *If the process for identifying risks is not performed in a systematic and structured manner, the Authority could fail to identify a risk which could have a very large financial and reputational impact.*	**LOW** ●

APPENDIX C

ISO 31000 Risk Management Policy Requirements

Absent requirements and rationale	Risk
A risk appetite statement The Authority should consider producing a Risk Tolerance and Appetite Statement to capture the amount and type of risk that it is willing to accept in order to achieve its Strategic objectives. The Authority should review this Risk Appetite Statement, which it sets in the context of WLWA's strategy and the regulatory framework, annually to provide the benchmark against which WLWA's risk profile is reported, monitored and managed within its risk governance structure.	*If the Authority's risk appetite is not clearly defined, management may have differing interpretations of what is considered an acceptable level in regards to residual risk potentially decreasing the likelihood of achievement of its operational and strategic objectives due to risks materialising or not being managed within acceptable tolerance.*
A list of documentation for analysing and reporting risk This will help to ensure a cohesive approach to risk analysis is undertaken as clear guidance on what documents the Authority requires services to use when analysing risk will be available to all staff members. Whilst, it will also ensure all staff members are aware of the correct reporting lines for emerging and deteriorating risks.	*Without clear guidance on the documentation required to analyse risk, a differing approach may be undertaken across the organisation, which could result in incorrect risk analysis. Whilst the absence of clear reporting lines may also lead to risks deteriorating and materialising.*
Risk activities and risk priorities for the coming year Documenting risk activities and risk priorities within the Risk Management Policy provides staff with further transparency to the potential risks ahead and aligns the Authority's Risk Management approach further with strategic aims. Whilst documenting these activities and priorities adds a level of accountability, ensuring they are undertaken during the year ahead.	*Without documenting the risk activities and priorities for the year ahead within the Risk Management Policy, there is a risk that an uncoordinated approach is taken and limited attention is focussed on these priorities and activities. This is turn could lead to emerging risks remaining unidentified, with other pre-identified risk deteriorating and materialising.*

APPENDIX D

INTERNAL AUDIT ASSURANCE LEVELS AND DEFINITIONS

Assurance Level	Definition
SUBSTANTIAL	There is a **good level of assurance** over the management of the key risks to the Authority's objectives. The control environment is robust with no major weaknesses in design or operation. There is **positive assurance** that objectives will be achieved.
REASONABLE	There is a **reasonable level of assurance** over the management of the key risks to the Authority's objectives. The control environment is in need of some improvement in either design or operation. There is a misalignment of the level of residual risk to the objectives and the designated risk appetite. There remains **some risk** that objectives will not be achieved.
LIMITED	There is a **limited level of assurance** over the management of the key risks to the Authority's objectives. The control environment has significant weaknesses in either design and/or operation. The level of residual risk to the objectives is not aligned to the relevant risk appetite. There is a **significant risk** that objectives will not be achieved.
NO	There is **no assurance** to be derived from the management of key risks to the Authority's objectives. There is an absence of several key elements of the control environment in design and/or operation. There are extensive improvements to be made. There is a substantial variance between the risk appetite and the residual risk to objectives. There is a **high risk** that objectives will not be achieved.

1. **Control Environment:** The control environment comprises the systems of governance, risk management and internal control. The key elements of the control environment include:
   - establishing and monitoring the achievement of the Authority’s objectives;
   - the facilitation of policy and decision-making;
   - ensuring compliance with established policies, procedures, laws and regulations – including how risk management is embedded in the activity of the Authority, how leadership is given to the risk management process, and how staff are trained or equipped to manage risk in a way appropriate to their authority and duties;
   - ensuring the economical, effective and efficient use of resources, and for securing continuous improvement in the way in which its functions are exercised, having regard to a combination of economy, efficiency and effectiveness;
   - the financial management of the Authority and the reporting of financial management; and
   - the performance management of the Authority and the reporting of performance management.

2. **Risk Appetite:** The amount of risk that the Authority is prepared to accept, tolerate, or be exposed to at any point in time.

3. **Residual Risk:** The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk.

APPENDIX D (cont’d)

RISK RESPONSE DEFINITIONS

Risk Response	Definition
TREAT	The probability and / or impact of the risk are reduced to an acceptable level through the proposal of positive management action.
TOLERATE	The risk is accepted by management and no further action is proposed.
TRANSFER	Moving the impact and responsibility (but not the accountability) of the risk to a third party.
TERMINATE	The activity / project from which the risk originates from are no longer undertaken.

INTERNAL AUDIT RECOMMENDATION RISK RATINGS AND DEFINITIONS

Risk	Definition
HIGH ●	The recommendation relates to **a significant threat** or opportunity that impacts the Authority's corporate objectives. The action required is to mitigate a substantial risk to the Authority. In particular it has an impact on the Authority’s reputation, statutory compliance, finances or key corporate objectives. **The risk requires senior management attention**.
MEDIUM ●	The recommendation relates to **a potentially significant threat** or opportunity that impacts on either corporate or operational objectives. The action required is to mitigate a moderate level of risk to the Authority. In particular an adverse impact on the Department’s reputation, adherence to Authority policy, the departmental budget or service plan objectives. **The risk requires management attention**.
LOW ●	The recommendation relates to **a minor threat or opportunity** that impacts on operational objectives. The action required is to mitigate a minor risk to the Authority as a whole. This may be compliance with best practice or minimal impacts on the Service's reputation, adherence to local procedures, local budget or Section objectives. **The risk may be tolerable in the medium term**.
NOTABLE PRACTICE ●	The activity **reflects current best management practice** or is an innovative response to the management of risk within the Authority. **The practice should be shared with others**.