

Risk & Audit Department

Olympic Delivery Authority

Report on General IT Controls

Reference Number – WP20

Overall Report Rating – ★★NEEDS IMPROVEMENT

May 2007

Contents

- EXECUTIVE SUMMARY 3**
 - OVERALL REPORT RATING 3
 - KEY FINDINGS 3
 - KEY ACTION ITEMS 6
- BACKGROUND..... 8**
 - CONTEXT 8
 - OBJECTIVES AND SCOPE 8
 - APPROACH..... 9
- A. GOVERNANCE 10**
- B. IT CONTROL ENVIRONMENT 16**
- C. THIRD PARTY MANAGEMENT 21**
- APPENDIX A: OVERALL REPORT RATING DEFINITION..... 25**
- APPENDIX B: RISK MATRIX CRITERIA 26**
- APPENDIX C: PRIORITISATION OF FINDINGS AND ACTION ITEMS 28**

Executive Summary

The objective of this audit was to examine the general IT control environment and assess whether it provides a reliable, secure and effective control framework for the processing of key information needed by the organisation and other stakeholders.

Overall Report Rating

This report has been given an overall report rating of “Needs Improvement” in accordance with the Risk & Audit report definition criteria as outlined in Appendix A. The “Needs Improvement” rating was assigned because of the number of major issues identified, particularly in relation to:

- consultation and communication between the business and IT department on programme decisions which have an IT impact
- the contractual arrangements with, and management of, third party contractors

Management were aware of these control weaknesses which may have resulted from the rapidly evolving operating environment and, prior to the audit, management had commenced some mitigation activities. However, we noted that whilst the overall assessment of the IT control environment relating to user access and change management was satisfactory, some minor process improvements were identified in this area.

Key Findings

There is insufficient communication between senior management and the IT department in relation to programme issues and decisions which may have an IT impact. As a result the IT department may not be fully aware of the impact on IT of decisions made at a high level, in a timely manner. Within the procurement and contract negotiation process there has been, and continues to be, limited involvement of IT specialists. Typically IT specialists have been consulted at a late stage or have not been fully integrated into the process. This has resulted in a lack of effective means by which the ODA can manage and monitor the third party contractors going forwards. We noted that there are a number of existing contracts which have inadequate clauses relating to IT governance, such that the ODA may encounter problems in the future with regard to enforcement of policies and procedures, and rights of access to gain assurance that adequate IT controls are in place.

In addition, the ODA has not yet put in place a framework of policies and procedures relating to the management and monitoring of third parties, from an IT perspective. Going forwards, this may result in inconsistencies and informality in the processes for managing third parties, increasing the likelihood of non-compliance with ODA IT policies and procedures.

Governance of IT, in particular the IT strategy and budgeting process, is not robust. The IT Governance arrangements are in the process of being negotiated with CLM, the Delivery Partner. The roles and responsibilities of the ODA and CLM IT departments are still to be agreed, with initial indications of ODA IT retaining responsibility for internal IT and provision of advice to the programme at a project sponsor level. We noted that the IT budget is developed without full consideration of the detailed costs and alignment with a formal IT strategy. A draft IT strategy (ODA IT Vision) document was developed in 2006 however, this was not approved. This strategy has a number of deficiencies and has not been updated to reflect recent and significant organisation developments within the ODA.

Key Risks

The key risks identified during the course of the project are illustrated in the matrix below. ODA’s *Risk Management Framework* was used to rate the identified risks, and is outlined in Appendix B. The below matrix plots all the risks associated with findings described throughout the body of this report. The risks with an overall severity rating of major are summarised in the table below for your reference.

Risk Matrix

Consequence	Likelihood					Overall Risk Severity
	Rare	Unlikely	Possible	Likely	Almost Certain	
Fundamental						Fundamental
Major			C1, C2	A2, C3		Fundamental
Moderate		A3, A5, B1, B2	A1, A4			Major
Minor		B3				Moderate
Insignificant						Minor

Major Risks

Ref	Summary Finding	Summary Risk	Report Page Ref
A2	Lack of timely communication with IT.	There is a risk that business decisions may be made without full understanding of the associated IT related risks. Lack of timely communication may mean that IT is not fully aware of projects with an IT impact, or of potential issues which may impact the overall programme. This may result in the need to handle IT requests at short notice, potentially impacting IT work on other parts of the programme and potential unplanned and more expensive IT expenditure. In extreme cases, due to the lack of notice, it may not be possible to address the issues and provide adequate IT services and solutions to meet the organisational requirements.	P12
C1/C2	Limited IT contractual requirements in existing contracts and limited IT engagement in the procurement and contract negotiation process	ODA and its contractors may not comply with government legislation e.g., Freedom of Information Act (FOIA), Data Protection Act (DPA), as well as National Archive (TNA) requirements resulting in reputational impact and financial penalties. In addition, the third parties may not comply with ODA policies, procedures and standards. ODA may have limited remit to enforce IT policies and procedures on third party contractors, potentially resulting in IT control weaknesses and reputational impact, as well as increased costs and inefficiencies.	P21, 22
C3	Lack of processes and procedures for monitoring third parties	ODA may be unable to adequately manage and monitor third party contractors; potentially resulting in non-compliance with ODA policies and procedures, potentially resulting in security breaches and reputational impact.	P24

Key Action Items

Detailed action items are included throughout the body of this report. ODA’s *Risk Management Framework* was used to rate identified risks, and the criteria used to prioritise findings and action items is outlined in Appendix C. In addition, the below table provides a summary of the high priority action items.

Ref	High Action Items	Agreed Implementation Date	Primary Responsibility for Action Item	Secondary Responsibility for Action Item	Report Page Ref
A2	Whilst the IT department is making significant efforts to align its function to the business environment by assigning project managers to specific areas of the business, this approach should be formalised within the IT strategy document and communicated to stakeholders. The IT strategy document should include the IT department’s approach to communication, including its IT spend decision making process, to make this transparent to the wider organisation and to facilitate more timely consultation with IT.	June 2007	Dennis Hone, Director of Finance and Corporate Services	Simon Pitt, Head of IT	P12
A2	The IT department and wider ODA need to take joint responsibility to work together to communicate and consult on IT topics on a timely basis. This responsibility can be championed by the Director of Finance and Corporate Services, to raise awareness and promote the two way communication and engagement between the IT department and wider ODA, to facilitate the IT planning, procurement and budgeting process.	June 2007	Dennis Hone, Director of Finance and Corporate Services	N/A	P12
C1	ODA should finalise relevant IT policies and procedures and formally issue these to third party contractors as soon as possible.	July 2007	Dennis Hone, Director of Finance and Corporate Services	Simon Pitt, Head of IT	P21
C1	The IT requirements within existing contracts (other than the Remediation Demolition contract) and projects should be identified and, where considered relevant based on a formal risk assessment, arrangements should be put in place for monitoring the provision of these IT services by the third parties.	July 2007	Dennis Hone, Director of Finance and Corporate Services	Simon Pitt, Head of IT	P21

OLYMPIC DELIVERY AUTHORITY – GENERAL IT CONTROLS

Ref	High Action Items	Agreed Implementation Date	Primary Responsibility for Action Item	Secondary Responsibility for Action Item	Report Page Ref
C2	Procurement should engage IT within the procurement and contract negotiation process.	May 2007 and ongoing	Morag Stuart, Head of Procurement	Simon Pitt, Head of IT	P22
C2	The ODA IT department should continue liaising with the legal teams to identify and agree standard terms and contracts to enable adequate clauses in relation to IT to be included within contracts going forwards. The use of such clauses should be determined based on a review of the associated risks and benefits to the ODA so that a balanced and cost effective approach can be taken.	May 2007	Simon Pitt, Head of IT	Celia Carlisle, Head of Legal	P22
C3	Whilst contractors are contractually responsible for management of the IT services and solutions required to support the provision of procured services, IT management should assess the risks associated with the loss of data, or security breaches of contractor IT systems, and the level of oversight they should retain over the contractors' IT environments.	July 2007	Dennis Hone, Director of Finance and Corporate Services	Simon Pitt, Head of IT	P24
C3	IT should develop third party management and monitoring policies and procedures as soon as possible and implement these for key third parties. This should include the development of a third party audit plan, based on an assessment of associated risk.	July 2007	Dennis Hone, Director of Finance and Corporate Services	Simon Pitt, Head of IT	P24

Background

Context

The Olympic Delivery Authority (ODA) has been set up to deliver new venues and infrastructure in time for the 2012 Olympic and Paralympic Games (“London 2012”). The ODA works alongside the London Organising Committee for the Olympic Games and Paralympic Games (LOCOG) which will organise, publicise and stage the London 2012 Games. LOCOG and the ODA operate as discrete organisations, however they work closely together and share offices and Information Technology (IT) infrastructure.

The current IT environment at the ODA is under development. During the last 12 months IT related projects have been undertaken to assess and develop the IT infrastructure at the ODA. The IT environment is complicated as it must dovetail with CLM who are engaged to provide programme and project management experience and to implement a suite of supporting IT functions to achieve joint ODA/CLM objectives.

In April 2006, an Initial IT Security Situation Assessment was performed by Ernst & Young to understand the ODA’s current IT security requirements. This identified “quick wins” that the ODA should implement to improve its current IT security controls and “next steps” that the ODA should perform in order to further enhance and maintain its IT security controls as it evolves and develops over the coming year.

During the summer of 2006 a project was undertaken to identify the requirements and procure the ODA Back Office Systems and Services (BoSS). Following from this, Fujitsu have been selected to implement and manage the identified BoSS, with an expected delivery date of June 2007.

Objectives and Scope

This review examined the general IT control environment and assessed if it provides a reliable, secure and effective framework for the processing of key information needed by the organisation and other stakeholders.

The review examined the existence and operation of key controls since 1 April 2006 in the areas listed below.

The scope of this review was reduced to the extent that we were able to rely on ODA relevant controls assessed as part of the LOCOG external financial audit. The scope included the following areas:

- Overview of the IT function
- IT Governance
- Programme governance and management

- Third party management
- Access Controls
- Software / Systems Development
- System and Network Security Controls
- Problem and incident management
- Physical and Environmental Controls
- Back Ups, Contingency Planning and Disaster Recovery

Out of scope of this review were any controls or systems that have been implemented for LOCOG. Specifically, we did not perform a review of the Information Management systems which are being implemented for LOCOG, which are to be used by the ODA.

Approach

This project was conducted in accordance with the Risk & Audit Department's audit methodology. The approach included:

- Interviews with IT and business personnel responsible for applications within the user departments (as agreed with Simon Pitt, the nominated key contact within the ODA IT department).
- Review of external audit documentation of the IT control environment prepared as part of the LOCOG external audit, and confirmation of controls for the ODA through inquiry.
- Review of relevant, available documentation.
- Process or control walkthroughs were performed to help validate information gained through management discussions.

A. Governance

IT Governance helps provide stakeholders and IT management with comfort that IT is aligned to short and long term business goals and priorities. Effective IT Governance requires the support of senior management within an organisation, particularly when making business decisions that potentially have an IT impact. In making business decisions, IT related risks should be considered and decisions should be communicated to IT in a timely manner to enable IT management to adequately plan and budget for support and resource requirements. Underpinning effective IT governance is an up to date IT strategy. The IT strategy should be aligned to the organisation’s business strategy and should include areas such as the definition of IT principles that guide IT decision making, the current and future IT state and competencies, and the IT operating model and governance structure. In addition, the IT strategy should define the organisation’s transformation plan for achieving the desired future state of IT.

The ODA IT governance processes and operating environment is currently in a state of significant change. The ODA is currently working with CLM, their Delivery Partner, to negotiate and clarify the IT related roles and responsibilities of the ODA and CLM, IT Governance arrangements and an overall IT strategy. For the ODA, the time critical nature of the programme is a significant factor to consider in the IT Governance arrangements and decision making processes.

It is understood that the ODA IT department is to be responsible for the provision of the internal IT at the ODA and to provide advice, at a project sponsor level, regarding IT services and solutions within other areas of the programme. CLM will project manage IT implementation for Programme related IT. Management represented that an Integration Manager is being appointed to oversee the IT services and solutions to be provided for contractors on the Olympic Park.

Finding	Action Items	Management Response
<p>A1 IT Budgeting and Lack of IT Strategy</p> <p>IT budgeting and forecasting of IT spend is not currently aligned with an overall IT strategy. In 2006, the ODA developed an IT Strategy (ODA “IT Vision, Aim, Objectives and Key Principles Guidance for Third Party Contractors”), which remains in draft and has not been approved. Since this strategy was drafted, there have been significant developments (eg. appointment of CLM, appointment of Fujitsu to deliver back office systems). It is understood that this draft strategy document will now form the basis of a new ODA IT strategy which is being developed in conjunction with the Delivery Partner, CLM.</p>	<p>1. The IT Strategy should be modified to accommodate recent developments (eg, appointment of CLM and Fujitsu) and specifically extended to include the following:</p> <ul style="list-style-type: none"> • Governance of IT • Decision making processes, specifically in respect of investment • Alignment of ODA, CLM, Fujitsu and others in delivering IT projects and services. <p>In addition, the revised IT Strategy document should be approved by the EMB.</p> <p>This strategy should then be used to drive the IT</p>	<p>Primary Action Item Owner: Dennis Hone, Director of Finance and Corporate Services</p> <p>Secondary Action Item Owner: Simon Pitt, Head of IT</p> <p>Implementation Date: June 2007</p> <p>Comments:</p> <p>The ODA deferred the finalization of the IT strategy until certain strategies in many business areas were developed; and CLM had agreed and justified the business and IT programme in place. The current IT</p>

Finding	Action Items	Management Response
<p>Discussions about the approval of IT spend indicated that this is typically performed on a project by project basis. While scheduled projects may appear on the annual budget with an allocation, there are a large number of unscheduled projects for which IT spend is required to be approved and this is made via the Executive Management Board. It is understood that there is limited provision made within the IT budget for such unscheduled projects and that these are reviewed and approved on a case by case basis. This situation is understood to be common across the ODA as a result of the ODA being within the start up phases in 2006-07 and in the initial stages of working with CLM.</p> <p>In addition, IT spend is frequently subsumed within wider third party contracts and the ODA IT department may be unaware of the full cost of IT to the organisation. A clearer view of the cost of IT could be determined by reviewing the budgets in these contracts.</p> <p><i>Risks:</i></p> <p>Without adequate controls around the IT budget process and allocation, and lack of alignment with an overall IT strategy, there is an increased risk that IT demands on the overall budget may be higher than stakeholder expectations or else may result in reduced budget allocation to scheduled projects due to the uncertainty around unplanned projects and the need to retain a contingency budget. This is particularly of concern due to the number of IT projects identified within the work streams. Business cases for these IT projects may be developed and spend approved without a strategic view of the provision of IT services. This may lead to a fragmented and inefficient IT environment. Further complexity within the IT environment may arise due to the lack of visibility over IT spend within contracts.</p> <p><i>Risk Severity Rating: Moderate</i></p>	<p>budget and guide the IT project prioritisation and IT spend decision making process.</p> <ol style="list-style-type: none"> 2. Refer to recommendations from the Business Planning Review, relating to process improvements in the budget process and re-forecasting process. Such improvements can assist in obtaining clear oversight of the annual IT budget and monitoring performance against this. 3. Going forwards, a sufficient discretionary project budget should be allocated out of the agreed IT budget to fund unplanned IT projects and requirements. 4. To gain a clearer view of the cost of IT, the IT department should: <ul style="list-style-type: none"> • Actively engage in the Procurement process (refer to Finding B1) to gain oversight of proposed IT spend in contracts. • Review IT spend within existing third party contracts and projects and, where considered relevant based on risk assessment and resource prioritisation, arrangements should be put in place for the ODA to maintain oversight of the third party IT spend. <p><i>Action Item Priority: Medium</i></p>	<p>strategy and CLM/ODA programme of IT work will be updated and approved by the EMB.</p> <p>The IT Budget is an amalgamation of CLM and ODA activity with the Head of IT acting as Project Sponsor and CLM taking on the Project Manager role for programme support IT. For 2006/07 (start up) budget processes were by necessity based on broad estimates and affordability criteria, however the agreed programme of work between CLM and ODA now provides a factual basis for further budgeting.</p> <p>See responses to A2.</p>

Finding	Action Items	Management Response
<p>A2 Lack of Timely Communication with IT</p> <p>Based on our discussions with IT management, we understand that there have been occasions when there has been a lack of timely communication with IT. This has resulted in IT being informed, at short notice, of the requirement for the provision of IT services. For example, the provision of IT services to CLM staff who were relocated to Lee Valley sports centre and to the Galliford-Try Site Office.</p> <p><i>Risks:</i></p> <p>Without IT consultation at early stages in an initiative, there is a risk that business decisions may be made without full understanding of the IT related risks. Additionally, without timely communication and consultation of IT, there is a risk that the IT department may not be fully aware of and informed at an early stage of projects where there may be IT impact, or of potential issues which may impact the overall programme. The lack of IT involvement at early stages may also result in the need to handle IT requests at short notice, potentially resulting in resource being redirected from other tasks, impacting and delaying other parts of the programme and increasing the likelihood that IT services and equipment need to be procured at short notice. This may result in unplanned and potentially more expensive IT expenditure due to the short time scales. In extreme cases, due to the lack of notice, it may not be possible to address the issues and provide adequate IT services and solutions to meet the organisational requirements.</p> <p><i>Risk Severity Rating:</i> Major</p>	<ol style="list-style-type: none"> 1. Whilst the IT department is making significant efforts to align its function to the business environment by assigning project managers to specific areas of the business, this approach should be formalised within the IT strategy document and communicated to stakeholders (Refer to Finding A1). The IT strategy document should include the IT department’s approach to communication, including its IT spend decision making process, to make this transparent to the wider organisation and to facilitate more timely consultation with IT. 2. The IT department and wider ODA need to take joint responsibility to work together to communicate and consult on IT topics on a timely basis. This responsibility can be championed by the Director of Finance and Corporate Services, to raise awareness and promote the two way communication and engagement between the IT department and wider ODA, to facilitate the IT planning, procurement and budgeting process. <p><i>Action Item Priority:</i> High</p>	<p>Primary Action Item Owner: Dennis Hone, Director of Finance and Corporate Services</p> <p>Secondary Action Item Owner: Simon Pitt, Head of IT</p> <p>Implementation Date: June 2007</p> <p>Comments:</p> <p>CLM and ODA IT have agreed a governance structure for IT and are in the process of finalising an “IT Strategy and Work Programme” for presentation to the ODA EMB on 16 May 2007.</p> <p>The Director of Finance and Corporate Services has already taken action to set up a working group to effectively embed IT and other corporate functions into appropriate decision making processes.</p>

Finding	Action Items	Management Response
<p>A3 Existence of Draft IT Policies and Procedures</p> <p>A number of the ODA policies and procedures eg, the Information Systems Acceptable Use Policy - Code of Practice, Dormant Account Policy, and Disaster Recovery policy, have been drafted but not finalised and approved. At the time of the audit, the ODA were in the process of reviewing the ODA policies and procedures to make them more applicable to the ODA situation with regard to reliance on third party contractors. The IT department has recently recruited an IT security manager who is revising these to reflect the ODA’s role and that of the third party contractors.</p> <p>We also noted that staff and contractors do not currently receive IT induction and awareness training.</p> <p><i>Risks:</i></p> <p>If these documents are not finalised and approved, ODA staff and contractors may not comply with the policies and procedures. This may result in, for example, weaknesses in IT security arrangements, inappropriate use of the IT systems by staff and contractors and inadequate provision of disaster recovery services.</p> <p><i>Risk Severity Rating: Moderate</i></p>	<ol style="list-style-type: none"> 1. The policy and procedure documents should be finalised and approved at the earliest opportunity and should be issued to third party contractors. 2. IT induction and awareness training should be performed for staff and contractors. The Information Systems Acceptable Use Policy - Code of Practice should also be issued to ODA staff and contractors and they should be required to sign up to agree that they will comply with this. <p><i>Action Item Priority: Medium</i></p>	<p>Primary Action Item Owner: Simon Pitt, Head of IT Secondary Action Item Owner: N/A</p> <p>Implementation Date: May 2007</p> <p>Comments: Policies will continue to be revised in line with the changing business environment. An updated Information Security Policy is now in place. This policy was approved by the Information Security Working Group on the 13/4/07. As from April 2007, all induction packs contain an Information Security Awareness Booklet. All new inductees (both permanent and contractors) will be shown an Information Security presentation as part of their roles. In addition, an Information Security Awareness Programme is being developed to educate all staff permanent and contractors.</p>

Finding	Action Items	Management Response
<p>A4 Regulatory Compliance Policies and Procedures</p> <p>The ODA policies and procedures in relation to compliance to the Freedom of Information Act (FOIA) were approved by the ODA Board at the Board Meeting on 25 January 2007. Although key staff handling FOIA requests were aware of the approved FOIA policies and procedures, there was limited circulation of these policies and procedures to staff generally. In addition, the ODA policies and procedures for compliance with the Data Protection Act (DPA) had not yet been finalised and approved. Whilst training and awareness had been provided to ODA employees and contractors in 2006, some staff eg. new joiners, may be unaware of the procedures to follow in relation to the FOIA and DPA.</p> <p><i>Risks:</i></p> <p>There is a risk that employees and contractors of the ODA may receive requests for information but may be unaware of their significance and hence appropriate action may not be taken within the timescales required. This may result in breaches of the FOIA and the DPA, potentially resulting in legal action against the ODA.</p> <p><i>Risk Severity Rating: Moderate</i></p>	<ol style="list-style-type: none"> 1. Regular training and education sessions should be held to increase staff awareness of the FOIA and DPA and their responsibilities in relation to the acts. 2. Policies and procedures relating to the acts should be finalised, where applicable, and circulated to staff, as appropriate. <p><i>Action Item Priority: Medium</i></p>	<p>Primary Action Item Owner: Celia Carlisle, Head of Legal</p> <p>Secondary Action Item Owner: Pieter De Waal, Project Manager - Legal</p> <p>Implementation Date: July 2007</p> <p>Comments:</p> <p>The ODA are updating the intranet procedures and are also adding an easy to use step-by-step handling procedure. There is a Freedom Of Information (FOI) help page for staff on the intranet which is to be more visible and easier to read when the Intranet is redesigned. There is an FOI page on the external website and requests are routed to the Communications department to be assessed and managed. This is to be made more prominent when the website is redesigned.</p> <p>As a result of a change of personnel handling the FOI requests in the Communications team, processes were formalised and improved with assistance from the Legal team. A dedicated FOI resource is to be appointed within the legal team who will take over the responsibility for FOI administration and processing. The processes may then need some minor adjustment.</p> <p>Further FOI staff training is planned. This will be performed by the Legal and Communications teams. The presentations have already been prepared. There are also plans to raise FOIA awareness via input into the HR "arrivals manual" for new joiners.</p> <p>The ODA has recently appointed a Records Manager and they will take on responsibility for Data Protection Act (DPA) compliance, including the development of policies and procedures. It is expected that DPA awareness will be incorporated into the awareness programme for FOI.</p> <p>The implementation date of July 2007 is dependent on website re-launch and how quickly the legal department is able to acquire the additional resource.</p>

Finding	Action Items	Management Response
<p>A5 Scope for Improving IT Project Management Processes</p> <p>The approach to managing IT projects is an area that has been under development over the last twelve months. Scheduled projects appear in the approved budget and a spreadsheet is maintained of smaller projects. The documentation of the projects is an area that is being improved, with the Project Manager now requiring scoping documents, approved budgets and Project Closure reports, requiring sign off from key stakeholders. At the time of the audit, the process had not been formally documented and approved, and was not being consistently applied.</p> <p><i>Risks:</i></p> <p>Without clear tracking and documentation of project scope and closure, there is a risk that the scope, risks and interdependencies of IT projects may not be clear and may not meet the project sponsor’s requirements, with potential financial and time implications.</p> <p><i>Risk Severity Rating: Moderate</i></p>	<ol style="list-style-type: none"> 1. We support IT management in formalising their approach to managing IT projects consistently. There is scope for improvements in the tracking and documentation of IT projects. IT management should formalise the IT project process (including EMB approval) to clarify the documentation requirements for individual projects, and should review compliance with this process on a periodic basis. 2. For budget review and audit purposes (Refer to Finding A1), IT management should consider retaining a log of those scheduled and unscheduled projects that have been completed and formally closed. <p><i>Action Item Priority: Medium</i></p>	<p>Primary Action Item Owner: Simon Pitt, Head of IT</p> <p>Implementation Date: May 2007</p> <p>Comments:</p> <p>The comments are taken positively. Historic projects may not have had all formal documentation in place – a conscious decision was taken to not “back date” this documentation as many of the “projects” were small internal “packets of work” with no external costs or low impact.</p> <p>All new Projects should comply with a formal PID and PCR. The definition of an IT “project” needs clarification. It is agreed that an “IT Project Process” summary document be drawn up to help clarify the processes, definitions, reporting requirements and project initiation, tracking and closure.</p>

B. IT Control Environment

The ODA IT environment is currently undergoing significant change, with CLM, the Delivery Partner, expected to take on a significant role in the delivery of IT services to the ODA going forwards. The IT solutions currently in use at the ODA are interim arrangements, involving significant use of spreadsheets, which are expected to be replaced during the next twelve months.

The ODA is currently in the process of implementing a Back Office System and Service, in conjunction with the third party, Fujitsu. As such the OpenAccounts finance application is to be replaced by Oracle Financials. This system is also to replace the existing IT solutions supporting the HR and procurement processes. CLM is also planning to implement Active Risk Manager to replace the existing spreadsheets that support the Risk Management process. Other planned system implementations include the Electronic Document and Records Management (EDRM) system and Enterprise Content Management system which are expected to be implemented in 2007.

Finding	Action Items	Management Response
<p>B1 Weak User Access Controls</p> <p>Within OpenAccounts, a number of weaknesses in user access controls were identified. It is understood that issues were also identified in the “Banking, Receipt and Payment review”. Whilst remediation was put in place following that review, these new processes need to be embedded and incorporated into day to day joiner, leaver and mover processes:</p> <ul style="list-style-type: none"> • There are no formalised procedures for authorising new users, amending their access levels or deleting user profiles when an employee changes role or leaves the organisation. • There are weaknesses in the password controls, such that users are not required to change their password on first login and there is no minimum length or password complexity enforced due to limitation in the application. • There is no segregation of duties between the roles for user administration and the review of user access. • A number of generic profiles and accounts (i.e. 	<p>1. We understand that the OpenAccounts system is to be replaced by Oracle Financials and that through this implementation the issues identified in relation to OpenAccounts, in both this review and the “Banking, Receipt and Payment review” are to be addressed. However, Finance should:</p> <ul style="list-style-type: none"> • Confirm interim controls are consistently implemented until Oracle controls are operating. • Segregate the roles of user administration and review of user access. • On a periodic basis, review user access to validate that the access rights to the IT systems and network remain in line with users’ job roles and to identify redundant accounts. • Review the user accounts and profiles present within the system and disable/remove those which are not necessary for the operation of the application and are not used by the business. This is particularly important due to the implementation of the new Oracle system to reduce the likelihood that, during the 	<p>1. Primary Action Item Owner: SianWilliams, Head of Finance Secondary Action Item Owner: N/A</p> <p>Implementation Date: May 2007</p> <p>Comments: The Financial Systems Accountant is to train another member of the team, the Financial Controller, to run the reports for the review of user access. Having two people skilled to run the necessary reports will facilitate consistent and ongoing control implementation. The Financial Controller will also review the reports on a monthly basis and pass to the Head of Finance for formal sign off. Management have reviewed the identified redundant accounts, and identified the following:</p> <ul style="list-style-type: none"> • Demo: (Demonstration User): This is used for the TEST environment, and Open Accounts help desk use when helping sort any problems (proxy in).

Finding	Action Items	Management Response
<p>accounts not owned by a single person) are present within the application.</p> <p>We also noted that there are no formal processes around the removal of users at the network level. This includes the access controls for the private directories for the individual departments. In addition, the access to the Private directories is not reviewed on a periodic basis.</p> <p>We noted that, at the time of the audit, there were three users on the access control list for the Procurement department, who had left the organisation over 25 days previously, one of whom was a user unknown to the Head of Procurement and the Procurement Manager. In mitigation, a dormant account policy is enforced, which requires accounts that have not been used for 21 days to be disabled.</p> <p><i>Risks:</i></p> <p>The risks arising from weak user access controls:</p> <ul style="list-style-type: none"> • It may be possible for someone to request a user account to be set up in relation to a different job role or function to their own, thus resulting in users being granted an inappropriate level of access to the system, or leading to circumvention of segregation of duties controls. • Without user termination and regular user access review processes, there is a risk that redundant profiles may be left on the system for a period after an employee has left the organisation or users may have excessive access rights to data held on the systems, thus creating an exposure to unauthorised access attempts and data modification. This leads to an increased risk of fraud, loss of service of IT systems, and financial loss. This is particularly of concern due to the large number of contractors within the ODA. • Weaknesses in password controls can compound the risks associated with deficiencies in the user access removal processes. • The lack of segregation of duties between the user administration and access review processes 	<p>implementation process, additional user accounts are not set up.</p> <ol style="list-style-type: none"> 2. IT should formally establish and communicate procedures for terminating a former employee’s access to the organisation’s systems and network. The IT team and system administrators should be promptly informed when an employee leaves the organization. This procedure should be accompanied by the appropriate supporting documentation. 3. With the implementation of Oracle, IT should take the opportunity to introduce formal access control procedures and enforce password controls in line with the ODA IT Security policy for the Oracle system. We understand that due to the current size of the finance function of the ODA, it has been possible to communicate user administration changes for OpenAccounts by word of mouth. However, as the organisation grows, these procedures become more unmanageable. The new Oracle system is to support business processes within multiple departments, including HR, procurement, as well as finance. Therefore, the user base for Oracle will be larger and more complex, increasing importance of implementing strong user access controls around the new system. User access requests can take the form of emails or be made on a standard form, authorised by specified individuals within individual departments and should be retained by the appropriate systems administrator as an audit trail. <p><i>Action Item Priority:</i> Medium</p>	<p>Password on Demo will only be known to systems accountant.</p> <ul style="list-style-type: none"> • NAO1: set up for NAO. Management discussed this account with NAO but as the account cannot be used to edit anything they felt it is ok. • POP1, POP2: These accounts have now been deleted <p>The Financial Systems Accountant will put in place a process for new user requests, a form will be completed and then signed by Head of Finance before user is set up.</p> <p>2 & 3. Primary Action Item Owner: Simon Pitt, Head of IT</p> <p>Secondary Action Item Owner: N/A</p> <p>Implementation Date: August 2007</p> <p>Comments:</p> <p>Oracle Finance will go live in June 2007, single sign on to Oracle via active directory will be implemented by August 2007. This will centralise the administration of access controls within the IT Team. The processes which are applied to all other user access to ODA systems will then apply.</p> <p>The leavers process has been in place for some time and has operated centrally for all systems other than Cedar Open Accounts. However processes will be formalised across ODA.</p>

Finding	Action Items	Management Response
<p>permits the user administrator to grant themselves or other users' unauthorised privileges within the system and then remove the corresponding entries from the access/activity report. Such access, and potential associated malicious activity, may then go unnoticed by management. This may lead to the confidentiality and integrity of business information being compromised and loss of system availability. This increases the risk of sabotage, damage to reputation and potentially financial loss and fraud.</p> <ul style="list-style-type: none"> • If someone is able to directly log into a generic account, as this is not assigned to an individual, there is reduced user accountability for activities performed. This may encourage unauthorised and malicious activity and the lack of accountability means that it is difficult to identify and stop those causing errors or irregularities. <p><i>Risk Severity Rating: Moderate</i></p>		

Finding	Action Items	Management Response
<p>B2 Lack of Logging and Monitoring of Log Files on OpenAccounts Server</p> <p>We noted that on the CPAP01 server hosting the OpenAccounts application that the ‘Audit Object Access’ function is not enabled. Security logs are cleared too frequently and there is no regular review of the security logs. In addition, system audit logs are not reviewed on a regular basis.</p> <p><i>Risks:</i></p> <p>If comprehensive audit logs are not maintained and reviewed, there is an increased risk that unauthorised activity may not be detected and addressed in a timely manner.</p> <p>Failure to retain log files for an adequate period of time increases the risk that unauthorised activity may not be traced at a later date or may result in system failures being untraceable, preventing the identification and correction of problems or security incidents in an accurate or timely fashion. The lack of evidence may also negatively impact upon the success of disciplinary action or criminal prosecution of an individual undertaking unauthorised activity.</p> <p>Failure to review audit logs in a timely manner increases the risk of unauthorised access to server resources being undetected for an extended period of time. Lack of monitoring gives a potential intruder sufficient time to find a weakness in security and potentially obtain access to sensitive data and programs.</p> <p><i>Risk Severity Rating: Moderate</i></p>	<ol style="list-style-type: none"> 1. IT should enable the ‘Audit Object Access’ function to facilitate monitoring of critical files and directories. 2. IT should implement procedures for the regular review of security and audit logs for the critical application servers. 3. Log retention policies should be adjusted to assist with such reviewing. Logs should be backed up and archived on a regular basis depending on the business requirements and size of log files. <p><i>Action Item Priority: Medium</i></p>	<p>Primary Action Item Owner: Simon Pitt, Head of IT Secondary Action Item Owner: N/A</p> <p>Implementation Date: June 2007</p> <p>Comments:</p> <ol style="list-style-type: none"> 1. We have reviewed the auditing and log capture on the Open Account system, taking into account the recommendations below and raised an RFC to address this. The action was completed on 9 April 2007. 2. There is a current project to centralise the correlation and monitoring of all logs. In the meantime, we have created a Log Review spreadsheet for log reviews on Open Accounts and, other critical and mission critical systems. 3. Audit Logs recording user activities, exceptions, and information security events have now been implemented as appropriate and kept for an agreed period to assist in future investigations and access control monitoring. Logs will be kept securely and access to logs managed and monitored. Log retention is covered in our Information Security Policy (Section 10.10).

Finding	Action Items	Management Response
<p>B3 Non-compliance of Account Lockout Settings with Security Policy</p> <p>We noted that account lockout is set to 4 invalid logon attempts, which is not compliant with the ODA IT Security Policy which details that account lockout should be set to 3 invalid logon attempts.</p> <p>Industry good practice is to set network accounts to lockout or delay further logon attempt after three invalid logon attempts. We understand that the ODA IT Security Policy also stipulates that this value.</p> <p><i>Risks:</i></p> <p>Failure to implement the defined account lockout increases the risk of an unauthorised individual being able to compromise the system by executing a brute force “dictionary” attack against user accounts. Such attacks are used to attempt to guess user passwords and gain unauthorised access to the IT systems, potentially resulting in disclosure of sensitive information or violating the integrity of the data.</p> <p><i>Risk Severity Rating:</i> Minor</p>	<p>1. IT should change the Default Domain Policy configuration to be in line with the ODA Security Policy.</p> <p><i>Action Item Priority:</i> Low</p>	<p>Primary Action Item Owner: Simon Pitt, Head of IT Secondary Action Item Owner: N/A</p> <p>Implementation Date: April 2007</p> <p>Comments:</p> <p>Completed. A Change was raised in order to rectify this situation as soon as the issue was raised. We are grateful to internal audit for identifying this issue, which was immediately rectified.</p>

C. Third Party Management

Ineffective control and management of third party contracts in relation to IT may have both financial and security implications. The ODA is in the process of negotiating many contracts that may have IT implications. As such, it is expected that there would be consideration of IT, and consultation of IT specialists, during the procurement and contract negotiation process. It is understood that some of the contracts, that have already been agreed and signed, do not include full consideration the IT related contractual requirements e.g., for rights of audit over the third party, enforcement of compliance with ODA policies and procedures and government regulatory requirements. Other contracts are currently in negotiation, or are to be negotiated in the immediate future.

Finding	Action Items	Management Response
<p>C1 IT Contractual Requirements in Existing Contracts</p> <p>Following our review of the LDA Legacy Remediation-Demolition contract, we noted that there are no contractual clauses relating specifically to IT. For this contract, we are aware that there is a significant budget allocation for IT, worth £1 million, for the provision of onsite IT services for a site office. The ODA has little control either over this IT spend or the subcontractor who has been appointed to provide the IT services. We understand that there was no due diligence performed in relation to the appointment of the IT subcontractor and that it is understood that they do not have experience within the government sector and are not aware of the specific requirements in relation to this. It was noted during our review that IT service performance issues arising from power cuts have already been experienced at the site office.</p> <p>Furthermore, we understand that there is no disaster recovery provision for the IT services that are being provided to the site office under this contract.</p> <p>We understand that the ODA IT department is discussing the IT service provision and the need to comply with the ODA standards and this is currently taking place out of good will on the part of the</p>	<ol style="list-style-type: none"> As noted in Finding A3, the ODA should finalise, where necessary, relevant IT policies and procedures and formally issue these to the contractor as soon as possible. The IT requirements within other existing contracts and projects should be identified and, where considered relevant based on a formal risk assessment, arrangements should be put in place for monitoring the provision of these IT services by the third parties. <p><i>Action Item Priority: High</i></p>	<p>Primary Action Item Owner: Dennis Hone, Director of Finance and Corporate Services</p> <p>Secondary Action Item Owner: Simon Pitt, Head of IT</p> <p>Implementation Date: July 2007</p> <p>Comments:</p> <p>Following receipt of advice from ODA Legal the following policies and procedures were issued to the LDE legacy Remediation-Demolition contractors:</p> <ul style="list-style-type: none"> • Third Party Security Policy - draft • Third Party Security Assessment - final draft • Network Connection Agreement and Code of Connection - final draft • Information Security Policy - ODA final draft • Procedures - email access • Policy deviation - Risk acceptance form • Security Awareness handbook • Intranet Security model • Policy and Operating Procedure for London 2012

Finding	Action Items	Management Response
<p>contractor and subcontractor, as the contractual arrangements are such that the contractor has agreed to undertake responsibility for the providing the IT services required to fulfill their contract.</p> <p>It is understood that the ODA legal team has advised that there is a clause in the contract that requires the contractor to comply with policies and procedures that are issued to them.</p> <p><i>Risks:</i></p> <p>The ODA has little contractual control over the IT services being implemented at the site office as part of this contract. There is a risk that the contractor may not be willing to comply with the ODA policies, procedures and standards and it will be difficult for the ODA to enforce such compliance.</p> <p>The inability of the ODA to easily enforce the relevant policies, procedures and standards, particularly in relation to the need to demonstrate value for money from IT, may mean that the ODA aims are not met and may also mean that government legislation e.g. Freedom of Information Act (FOIA), Data Protection Act (DPA) and the National Archives (TNA) is not met. Without adequate rights of audit and agreement of SLAs and KPIs, the ODA may find it difficult to gain visibility of and monitor the quality of service and compliance with policies and procedures. This may result in additional cost and reputation implications.</p> <p><i>Risk Severity Rating: Major</i></p>		<p>IT Equipment Rooms v1_1</p> <ul style="list-style-type: none"> • Policy and Op Proc Access to Mailboxes v1_0 • Data Access Security Model v1_0 • Backup and Recovery Policy FINAL v1_0 • London2012 Dormant account policy Draft Version1.3 <p>A review of all other contracts is underway and will be completed by July 2007.</p> <p>See response to C3 for monitoring.</p>
<p>C2 IT Engagement in the Procurement and Contract Negotiation Process</p> <p>There is limited or no engagement of IT specialists during the procurement and contract negotiation processes. We noted that the ODA IT department has limited visibility over the procurement and contract negotiation process, and has had limited input to the contract drafting process to help bring consistency into</p>	<ol style="list-style-type: none"> 1. Procurement should engage IT within the procurement and contract negotiation process. 2. The ODA IT department should continue liaising with the legal teams to identify and agree standard terms and contracts to enable adequate clauses in relation to IT to be included within contracts going forwards. The use of such clauses should be determined based on a review of the associated 	<p>1. Primary Action Item Owner: Morag Stuart, Head of Procurement</p> <p>Secondary Action Item Owner: Simon Pitt, Head of IT</p> <p>Implementation Date: May 2007 and ongoing</p>

Finding	Action Items	Management Response
<p>contracts and include relevant IT contract clauses to enable effective control and visibility of third party contractors in relation to IT e.g. agreement of SLAs, KPIs, appointment of IT subcontractors, compliance with IT policies and procedures covering areas such as security, Freedom of Information Act (FOIA), Data Protection Act (DPA) and the National Archives (TNA) and value for money.</p> <p>We understand that multiple procurement and legal teams are working on various contracts and there is limited sharing of information and awareness of the importance of inclusion of IT consideration during the contract negotiation process.</p> <p>The IT department is currently working with the ODA and CLM legal teams to identify standard IT clauses that should be included in contracts going forwards.</p> <p><i>Risks:</i></p> <p>As evidenced in Finding C1, without the engagement of ODA IT specialists in the procurement and contract negotiation processes, there is a risk that the ODA has limited remit to enforce policies and procedures on the third party contractors, and appointed subcontractors. This may weaken the ability of the ODA to act in the role of the “intelligent client” and gain oversight of and effectively manage the contracts. As the number and complexity of contracts increases within the ODA, so does the ODA’s exposure to risks associated with those contracts. There is the potential that deficiencies within the contracts may result in increased costs and inefficiencies in relation to IT as well as risks to reputation and national security arising from breaches of security through non-compliance with ODA policies and procedures.</p> <p><i>Risk Severity Rating:</i> Major</p>	<p>risks and benefits to the ODA so that a balanced and cost effective approach can be taken.</p> <p><i>Action Item Priority:</i> High</p>	<p>Comments:</p> <p>The ODA has now developed standard contract terms relating to IT and has embedded relevant work instructions relating to IT in all contracts. The Procurement department is continuing to work with IT and other functions within the organisation to ensure consistency of process and true embedding of policies throughout all contracts.</p> <p>2. Primary Action Item Owner: Simon Pitt, Head of IT</p> <p>Secondary Action Item Owner: Celia Carlisle, Head of Legal</p> <p>Implementation Date: May 2007</p> <p>Comments:</p> <p>The ODA has now developed a set of documented procedures in relation to IT to be performed prior to entering into contracts with any third party services. Information security requirements are integrated into all third party contracts.</p>

Finding	Action Items	Management Response
<p>C3 Lack of Processes and Procedures for Monitoring Third Parties</p> <p>There are currently no IT related policies and procedures in place to manage and monitor third party contractor compliance with the contract and ODA policies and procedures.</p> <p><i>Risks:</i></p> <p>Without defined IT related policies and procedures for management and monitoring of third party contractors, there is a risk that, going forwards, informality and inconsistencies may be taken in the approach to monitor and manage third party contractors. This increases the likelihood of future non-compliance with contractual arrangements and ODA policies and procedures, potentially resulting in security breaches and reputational impact.</p> <p><i>Risk Severity Rating:</i> Major</p>	<ol style="list-style-type: none"> 1. Whilst contractors are contractually responsible for management of the IT services and solutions required to support the provision of procured services, IT management should assess the risks associated with the loss of data, or security breaches of contractor IT systems, and determine the level of oversight the ODA should retain over the contractors' IT environments. 2. IT should develop third party management and monitoring policies and procedures as soon as possible and implement these for key third parties. This should include the development of a third party audit plan, based on an assessment of associated risk, incorporating aspects such as: <ul style="list-style-type: none"> • Third party contractor risk assessments • Regular third parties self assessments of compliance with ODA policies and procedures • ODA compliance verification audits • Reporting on service quality and performance against SLAs and KPIs. <p><i>Action Item Priority:</i> High</p>	<p>Primary Action Item Owner: Dennis Hone, Director of Finance and Corporate Services</p> <p>Secondary Action Item Owner: Simon Pitt, Head of IT</p> <p>Implementation Date: July 2007</p> <p>Comments:</p> <p>Outsourced areas are integrated into the internal control system and there is a method of monitoring and controlling the third party service provider on an ongoing basis with regular reporting from the service provider. In addition, the ODA will regularly review and monitor the security practices and processes of the service provider, including performing periodic audits on the security adequacy and compliance of the service provider. Third party contracts include explicit security requirements, including incident response requirements.</p> <p>A third party contractor audit plan is under development and will be in place in July 2007.</p>

Appendix A: Overall Report Rating Definition

Overall report ratings are provided for each audit deliverable to indicate a general level of internal control, risk mitigation and performance. It is used by management to provide an overall indicator of report contents and severity of findings, which have been identified and require action.

Report Category	Report Category Summary	Report Category Definition
Excellent ★★★★★	Overall internal controls were in place, operating effectively and adequately mitigated key risks	Only a small number of minor or insignificant risks or control weaknesses were identified. Line management will address the low priority action items as, and when, required.
Good ★★★★	With limited exceptions, overall internal controls were in place, operating effectively and adequately mitigated key risks	A number of minor or insignificant risks and control weaknesses were identified, and, if taken together, may indicate a general weakness in the control environment to be addressed as a low priority. Line management will undertake actions to strengthen the control environment.
Satisfactory ★★★	Overall internal control and risk mitigation activities were satisfactory	A number of moderate and minor risks or control weaknesses were identified. Or, recognising the first year of operation of the ODA, some major risks with mitigation strategies were identified. These weaknesses may result in inefficient or ineffective resources, and a decrease in management control. Line Management will address identified action items within the agreed timeframes. Risk & Audit will apprise the Audit Committee of the status of agreed actions, and in particular when agreed implementation dates have not been met.
Needs Improvement ★★	Overall internal controls and risk mitigation activities require improvement	A number of major or moderate risks were identified. There were weaknesses in controls which could compromise or undermine management control, there were largely inefficient or ineffective use of resources, or there were risks which were not effectively mitigated. A number of high and medium priority action items were identified and will be addressed by Line Management within the agreed timeframes. Risk & Audit will apprise the Audit Committee of the status of agreed actions, and in particular when agreed implementation dates have not been met.
Unacceptable ★	Overall controls were not in place, operating effectively or mitigating key risks	A number of fundamental or major risks were identified. Either the design of controls did not appropriately mitigate identified risks, there were numerous indicators that controls were not functioning as designed, or there were largely inefficient or ineffective use of resources. A number of immediate and high priority action items were identified and will be addressed by Line Management as a matter of priority. Risk & Audit will apprise the Audit Committee of the status of agreed actions and in particular when agreed implementation dates have not been met.

Appendix B: Risk Matrix Criteria

The *ODA Risk Management Framework* requires risk severity to be determined using a five by five risk matrix. The tables below outline the likelihood and consequence assessment definitions used to facilitate categorising the risk severity of audit findings and risks.

Likelihood Risk Assessment Criteria

Likelihood Category	Likelihood Category Definition
Almost Certain	Expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Could occur at some time
Unlikely	Not expected to occur
Rare	May occur only in exceptional circumstances

Consequence Risk Assessment Criteria

Risk Group	CONSEQUENCE DEFINITION				
	Fundamental	Major	Moderate	Minor	Insignificant
Strategic	<u>Inability to deliver programme</u> , project or business objective	<u>Severe</u> impact on ability to deliver programme, project or business objective	<u>Significant</u> impact on ability to deliver projects or business objectives	<u>Material</u> impact on ability to deliver project or business objectives	<u>Little</u> impact on ability to deliver project or business objectives
Operations	Inaccurate or delayed information used in key <u>decision making</u> Inefficient or ineffective controls in a <u>critical</u> component of the control environment arising from, inter alia: resource management; information technology management; or asset and property management.	Inaccurate or delayed information used for <u>internal reporting</u> Inefficient or ineffective controls in a <u>significant</u> component of the control environment arising from, inter alia: resource management; information technology; management; or asset and property management.	Delays in obtaining accurate <u>management</u> information Inefficient or ineffective controls in a <u>material</u> component of the control environment arising from, inter alia: resource management; information technology management; or asset and property management.	Delays in obtaining <u>ad hoc</u> information Inefficient or ineffective controls in <u>some</u> components of the control environment arising from, inter alia: resource management; information technology management; or asset and property management.	Delays in obtaining <u>ad hoc</u> information in <u>isolated</u> instances Inefficient or ineffective controls in a <u>very minor</u> component of the control environment arising from, inter alia: resource management; information technology management; or asset and property management.
Compliance	Failure to comply with <u>critical</u> mandatory legal or regulatory requirements	Failure to comply with <u>mandatory</u> legal or regulation requirements	Failure to comply with a <u>mandatory</u> legal or regulation requirement in an <u>isolated</u> instance	Failure to comply with <u>recommended</u> legal or regulatory requirements	Failure to comply with a <u>recommended</u> legal or regulatory requirement in an <u>isolated</u> instance
Financial	Adverse impact on actual revenue or actual costs > £20 million NAO <u>audit qualification</u> on the reports or accounts	Adverse impact on actual revenue or actual costs between £10 - £20 million NAO raises <u>significant</u> control weaknesses or management issues	Adverse impact on actual revenue or actual costs between £5 - £10 million NAO raises <u>isolated</u> control weaknesses or management issues	Adverse impact on actual revenue or actual costs between £1 and £5 million NAO raises <u>process improvement</u> suggestions	Adverse impact on actual revenue or actual costs less than £1 million NAO raises <u>some low priority</u> process improvement issues

Appendix C: Prioritisation of Findings and Action Items

The following criteria has been used to prioritise findings and action items. The Risk Severity Rating has been derived from *ODA's Risk Management Framework* which uses a five by five risk matrix to define risk severity.

Risk Severity Rating	Finding & Action Item Priority	Priority Definition
Fundamental	Immediate	<ul style="list-style-type: none"> ▪ weakness which could <u>negate</u> management control and the ability to direct and manage ODA's business affairs ▪ weaknesses may result in <u>largely</u> inefficient or ineffective use of resources ▪ issues categorised as immediate could have the potential to <u>severely</u> impact the operation of the ODA
Major	High	<ul style="list-style-type: none"> ▪ weakness which could <u>compromise</u> management control and the ability to <u>adequately</u> direct and manage ODA's business affairs ▪ weaknesses may result in <u>significantly</u> inefficient or ineffective use of resources ▪ issues categorised as high could have the potential to <u>significantly</u> impact the operation of the ODA
Moderate	Medium	<ul style="list-style-type: none"> ▪ weakness which could <u>undermine</u> the system of management control, and the ability to demonstrate proper accountability, probity and openness in business operations ▪ weaknesses may result in inefficient or ineffective use of resources ▪ issues categorised as medium could have the potential to <u>materially</u> impact the operations of ODA
Minor or Insignificant	Low	<ul style="list-style-type: none"> ▪ weaknesses which could have a <u>minor</u> impact on the system of management control ▪ weaknesses may have a <u>minor</u> impact on the efficiency or effectiveness of processes or use of resources at present