Deloitte.

Imperial College

Internal Audit Report

Disaster Recovery – Research Departments Audit

Distribution List:

Arthur Spirling – Director of ICT
John Shemilt – Deputy Director of ICT and Head of Technology Operations
Professor Sir Peter Knight – Senior Principal of Imperial
Martin Knight – Chief Operating Officer (Final Report Only)
Rodney Eastwood – College Secretary (Final Report Only)
Andrew Murphy – Director of Finance (Final Report Only)

Date of fieldwork:	**May 2009**
Date of draft report:	**June 2009**
Date of final report:	**July 2009**

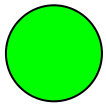
Contents

1. EXECUTIVE SUMMARY

1.1 Opinion

Based on the work undertaken as detailed in the 'Audit Objective and Scope', our overall assessment is that the classification of assurance in respect of the controls over the stated processes and systems is **substantial** assurance.

Full	Substantial	Limited	None



1.2 Rationale

We have made five Priority 2 recommendations where we consider controls may be further improved. The findings and recommendations are highlighted in the Observations and Recommendations Section.

The findings relating to the recommendations include:

- Establishing formal documented policies and procedures for the backup and recovery of research data;
- Establishing formal arrangements for the secure offsite storage of critical backup data and media;
- Improving the physical and environmental controls within the Mechanical Engineering (Mech Eng) and Huxley data centres*; and
- Investigation, documentation and regular testing of offsite disaster recovery arrangements for the replacement of hardware.

(*Where as part of the sample testing weaknesses were identified in specific research data centres and research departments these weaknesses were raised with the responsible party.)

1.3 Background

Imperial College are renowned for their research work undertaken in a number of areas. To aid in improving and maintaining their reputation, research is backed by the College's Research Strategy Office, which helps to formulate and communicate the College's research strategy and policy through strategic planning and consultation involving the College Strategic Research Committee. Significant investment has gone into building this reputation and the resulting research quality helps feed this reputation. Research data can be a very valuable asset to the College as well as to the sponsors, and as such, any unavailability of this data through loss, theft or damage could have a significant impact on the College reputation and standing in this area. It is therefore important that the College has assurance over the physical security of these assets and that, if there is a failure, the research data can be recovered within an acceptable time to the College.

Servers which hold Research data are generally managed by ICT. However, there are some servers located in the individual research departments, where their backup and recovery is the responsibility of the research department unless ICT have agreed to manage them.

The following risks from the Summary Risk Register were considered as part of this audit:

- Loss or theft of research data; and
- Loss of funding and damage to reputation as a result of loss of data and disaster.

1.4 Acknowledgement

We would like to thank all staff within ICT and the Research departments for their co-operation during the internal audit.

2. OBSERVATIONS AND RECOMMENDATIONS

2.1 Backup Policies and Procedures - Priority 2

Recommendation	Rationale	Responsibility
It is recommended that the Strategic Research Committee, in consultation with ICT, establishes and agrees formal documented backup and recovery policies and procedures for research data (Whether managed by ICT or individual research projects). The policy and procedures should include, but should not be limited to the: • Roles and responsibilities for the backup of research data; • Scope of the backups; • Frequency of backups; • Backup cycles in use; and • Daily operational procedures to be carried out (including monitoring for unsuccessful backups); and • Procedures for the periodic test restore of backup data. Furthermore, the policy and procedures should be reviewed and updated (if required) on an annual basis or whenever any major changes to systems take place.	Formal backup policies and procedures would provide a clear framework to help ensure that research data is backed up on a regular basis and that in the event of an incident/disaster, data loss is minimised and data may be restored in a timely manner. From a sample of seven research groups, it was identified that in all seven cases the research groups did not have any formal documented backup and recovery procedures in place. Furthermore, four of these groups stored their data on local hard drives which are not subject to any formal regular backup routines and therefore the backup of this data was reliant on the individuals concerned. There is a risk that backups may be inadequate which may result in a loss of research data, reputational damage to the College and/or adverse financial implications on the research grant.	See Management Response

Backup Policies and Procedures (Continued)

Management Response	Implementation Deadline
Agreed in principle	
The basic requirement to safeguard data is already enshrined in the "College Information Systems Security Policy" http://www3.imperial.ac.uk/ict/services/securitynetworkdatacentreandtelephonyservices/security/securitypolicies/policy/securitypolicyindex, as ratified by the Information Systems Security Group. Code of practice 2, Back-Up gives details of the approach but operational details are dependant on the data.	In place
Strategic Research Committee will be asked to endorse the College Information Systems Security Policy and publicise it.	Oct 2009
Strategic Research Committee has formed a sub group to ensure that suitable policy and procedures are in place for research groups.	April 2009
Details of ICT file storage and backup services are provided at the following URL: http://www3.imperial.ac.uk/ict/services/useremailfileanddirectoryservices/file_and_backup_services	In place
Details of the process of implementing the policy will vary depending on the value of the data to be protected and therefore it is inappropriate for this to be part of the policy. ICT will document best practice for backup with examples for reference by members of College.	Nov 2009

2.2 Storage of Backup Data and Media - Priority 2

Recommendation	Rationale	Responsibility
It is recommended that formal arrangements are made for the secure offsite storage of critical backup data and media. Details of secure off site storage arrangements should be included in the backup and recovery policies and procedures for research data recommended in recommendation 2.1.	Adequate offsite storage arrangements for backup data and media would help to reduce the likelihood of data loss and increase the ability to recover data in a timely manner. From a sample of seven research groups selected, it was identified that in six cases the offsite storage arrangements were inadequate. In most cases the backups were undertaken to removable storage media (USB stick, external hard drive, etc) and then taken offsite to the private residence of a researcher within the research group. Where offsite storage arrangements for backup data are inadequate, there is a risk that data loss may occur through damage and/or theft. Furthermore, there is a risk that recovery efforts may be delayed.	See Management Response

Storage of Backup Data and Media (Continued)

Management Response	Implementation Deadline
Agreed in principle The need to remotely store backup data off-site is already in the "College Information Systems Security Policy".	In place
ICT will make it part of its standard backup offering for backing up systems to ask system owners which of the current locations (Huxley or Hammersmith) they want their backups to be stored at.	Oct 2009
Strategic Research Committee will be asked to endorse the College Information Systems Security Policy and publicise specifically Code of Practice 2: Contingency Planning/ Disaster Recovery.	Oct 2009
Off-site storage for physical media storage is not currently provided. The Strategic Research Committee sub group will consider the viability of this and make a recommendation on the way forward.	April 2010

2.3 Physical Access Controls – Priority 2

Recommendation	Rationale	Responsibility
Research groups should be encouraged to utilise the main ICT data centre for hosting and managing their servers. However, where research groups decide to host and manage their own servers, management should ensure that adequate physical controls are in place, and backups managed as per recommendation 2.1. It is also recommended that ICT management consider implementing the following physical access controls within the ICT Server Rooms: • Burglar alarms linked to College security should be installed within the Mech Eng and Huxley Research data centres; • Visitors to the Huxley data centre should be required to sign in/out of a visitors register; • Cabling within the Huxley data centre should be protected by trunking and/or overhead trays; and • CCTV, connected to College security, should be installed in and around the Huxley data centre.	Physical access controls will help to ensure that loss/damage to computer equipment installed within the data centre(s) is minimised. It was identified that: • Burglar alarms have not been installed within the Mech Eng and Huxley data centres; • Visitors to the Huxley data centre are not required to sign in/out of a visitors register; • Cabling within the Huxley data centre is not always protected by trunking and/or overhead trays; and • There is no CCTV, connected to College security, installed in and around the Huxley data centre. There is a risk of unauthorised access and damage to computer equipment and/or data storage media.	See Management Response

Physical Access Controls (Continued)

Management Response	Implementation Deadline
Agreed in principle	
Mech Eng is currently fitted with a door alarm and one for Huxley is on order as part of the swipe card lock.	Aug 2009
Physical security is covered by code of practice 5, “Physical Security of Information Systems” where security measures appropriate for the value should be taken.	In place
Strategic Research Committee will be asked to endorse the College Information Systems Security Policy and publicise specifically Code of Practice 5: Physical Security of Information Systems.	Oct 2009
The future of the Department of Computing data centre is currently unclear and until its future is resolved it will influence investment in it.	
ICT will obtain quotes for the fitting of alarms to both Huxley and Mech Eng data centre. Installation will be dependant on provision of funding.	Oct 2009
ICT will obtain a quotation for fitting CCTV in around the Huxley data centre. Installation will be dependant on provision of funding.	Oct 2009
Department of Computing will provide a visitors book for the Huxley data centre.	Oct 2009

2.4 Environmental Controls - Priority 2

Recommendation	Rationale	Responsibility
Research groups should be encouraged to utilise the main ICT data centre for hosting and managing their servers. However, where research groups decide to host and manage their own servers, management should ensure that adequate environmental controls are in place, and backups managed as per recommendation 2.1. It is also recommended that ICT management consider implementing the following environmental controls within the ICT Server Rooms: • An automated fire suppression system should be installed within the Mech Eng and Huxley and data centres; • A standby alternative power supply (e.g. generator) should be installed with the Mech Eng and Huxley data centres; • The hand held fire extinguishers within the Mech Eng data centre should be maintained on a regular basis (at least annually); • Water detection sensors should be installed within the Huxley data centre; • The Huxley data centre should be cleaned on a regular basis and any non data centre related items removed; and	Effective environmental controls help to minimise the probability and impact of disruptions to the IT service. The following weaknesses were identified: • Automated fire suppression systems have not been installed within the Mech Eng and Huxley data centres; • There is no alternative power supply available for the Mech Eng and Huxley data centres; • Eight of the nine hand held CO2 fire extinguishers identified within the Mech Eng data centre had not had a maintenance check within the last year; • Water detection sensors have not been installed within the Huxley data centre; • The Huxley data centre is not being maintained as clean and tidy; and There is an ongoing risk of system disruptions and data loss due to weaknesses in environmental controls in the data centre.	See Management Response

Environmental Controls (Continued)

Management Response	Implementation Deadline
Agreed in principle • Fire suppression has been considered and rejected due to cost. ME data centre has a Vesda system to give early indication of fire. • UPS are used to allow graceful shutdown where justified. Retrofitting of generator backup is not justified on cost grounds, though for the Mech Eng data centre emergency power connections will be looked at allowing a mobile generator to be used. Future data centre builds will consider generator provision. • It has been confirmed with the Chief Fire Officer that the fire extinguishers in the Mech Eng. Data Centre are maintained on an annual basis and the date on them is not the expiry date but the inspection date. • DoC and ICT will work together to improve the cleanliness of Huxley data centre and form a joint team to take this and other aspects forward • The Huxley Data Centre does not use a water based cooling system and therefore under floor water detection is not necessary.	Spring 2010
Imperial College policy is not to have research group data centres. Strategic Research Committee will be asked to endorse this policy and remind Departments and research groups.	Oct 2009

2.5 Disaster Recovery Arrangements - Priority 2

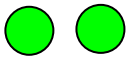
Recommendation	Rationale	Responsibility
It is recommended that offsite disaster recovery arrangements for the replacement of hardware are investigated, documented and regularly tested.	Recovery arrangements for the replacement of hardware would help to ensure that the College is able to restore critical services in a timely manner. It was identified that the College does not currently have any alternative disaster recovery arrangements in place for the recovery of hardware. There is a risk that the College may be unable to restore critical services within expected timeframes.	See Management Response

Management Response	Implementation Deadline
Agreed in principle It is a requirement of the College Disaster Recovery planning that this is considered and is included in the "College Information Systems Security Policy". ICT does currently have access to multiple data centres on the South Kensington campus however this does not protect against a disaster affecting the whole of this campus.	
Possibilities for another data centre not on the South Kensington campus are being considered. A paper has already been presented to the CEO detailing the requirements.	In place
Arrangements for alternative hardware are considered on a value basis. ICT has spare systems for some of the most important services.	Continual

APPENDIX A - REPORTING DEFINITIONS

Assurance Gradings

We have four categories by which we classify internal audit assurance over the processes we examine, and these are defined as follows:

Assurance Level	Evaluating and Testing Conclusion
Full 	The controls in place adequately address all risks identified and all controls tested are operating effectively.
Substantial 	The controls in place adequately address all significant risks identified and all key controls tested are operating effectively.
Limited 	The controls in place do no adequately address one or more significant risks identified and/or one or more key controls tested are not operating effectively.
None 	The controls in place do not adequately address several significant risks identified and/or the key controls tested are not operating effectively, resulting in unnecessary exposure to risk.

The assurance gradings provided above are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Full Assurance' does not imply that there are no risks to the stated objectives.

Recommendation Gradings

In order to assist management in using our internal audit reports, we categorise our recommendations according to their level of priority as follows:

Priority Level	Definition
1	Major issues for the attention of senior management and the audit committee.
2	Important issues to be addressed by management in their areas of responsibility.
3	Minor issues resolved on site with local management.

3. APPENDIX B – AREA OBJECTIVE AND SCOPE

This internal audit forms part of the agreed 2008/09 Internal Audit plan as approved by the Audit Committee on 11 June 2008.

The overall objective of this internal audit was to provide the Governing Body, the designated officer and local management with reasonable, but not absolute, assurance as to the adequacy and effectiveness of the key controls relating to the following objectives:

- Backup Regime - To ensure that adequate arrangements are in place to allow for the backup of data on a regular basis. To ensure that backup data is complete and reliable;
- Recovery Arrangements - To ensure that adequate arrangements are in place for the timely recovery of systems used by research departments; and
- Physical and Environmental Controls - To ensure that adequate physical and environmental controls are in place to help protect the servers in the research departments.

4. APPENDIX C - STAFF INTERVIEWED

John Shemilt	Deputy Director of ICT and Head of Technology Operations;
Paul Allatt	ICT Link Manager;
Steve Lawlor	Data Centre Manager;
Steve Kellock	Senior Research Officer, Space and Atmospherics Physics Group;
Dr Peter Slootweg	Research Officer, Space and Atmospherics Physics Group;
Jo McHugh	Research Centre Manager, Innovation Studies Centre;
Dr John de Mello	Reader in Nanomaterials, Nanostructured Materials and Devices Group;
David Botschinsky	Computer Manager, Kennedy Institute of Rheumatology;
Prof Richard Thomas	Professor of Pure Mathematics, Pure Mathematics;
Emeritus Prof Geoffrey Hewitt	Senior Research Investigator, Multiphase Fluid Systems Programme;
Dr Colin Hale	Research Fellow, Multiphase Fluid Systems Programme;
Dr Samia Girgis	Honorary Senior Lecturer, Investigative Medicine Department;
Prof Mike Warner	Professor, Department of Earth Science and Engineering.

5. APPENDIX D - AUDIT OBJECTIVE AND SCOPE

The objective of the audit was to determine whether management have implemented adequate and effective controls over the arrangements with regards to the backup and recovery of research data.

The audit approach was developed through an assessment of risks and management controls operating within each area of the scope.

The following procedures were adopted:

- Identification of the role and objectives of each area;
- Identification of risks within each area which threaten the achievement of objectives;
- Identification of controls in existence within each area to manage the risks identified;
- Assessment of the adequacy of controls in existence to manage the risks and identification of additional proposed controls where appropriate; and
- Testing of the effectiveness of key controls in existence within each area.

Our audit focussed on the controls and processes within the following areas, as agreed with management:

- Backup Regime;
- Recovery Arrangements; and
- Physical and Environmental Controls.

6. APPENDIX E – RESTRICTIONS OF USE AND LIMITATIONS

As set out in our engagement letter, we wish to draw to your attention that this internal audit report may only be used in accordance with our engagement letter and not made available to third parties, except as may be required by law or for other statutory review bodies.

Management should be aware that our internal audit work was performed in accordance with the UK Government Internal Audit Manual standards which are different from audits performed in accordance with International Standards on Auditing (UK and Ireland) issued by the Auditing Practices Board. Similarly, the assurance gradings provided in our internal audit report are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Our internal audit testing was performed on a judgemental sample basis and focussed on the key controls mitigating risks. Internal audit testing is designed to assess the adequacy and effectiveness of key controls in operation at the time of the audit. Definitions of the assurance gradings and recommendation gradings used in this internal audit report are provided in Appendix A.

7. STATEMENT OF RESPONSIBILITY

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system. The assurance level awarded in our internal audit report is not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board.

Deloitte & Touche Public Sector Internal Audit Limited
London
June 2009

In this document references to Deloitte are references to Deloitte & Touche Public Sector Internal Audit Limited.