University of Glasgow

Internal Audit Update

2008/09 Annual Report

4th November 2009

This report and the work connected therewith are subject to the Terms and Conditions of the contract between University of Glasgow and Deloitte LLP. The report is produced solely for the use of University of Glasgow. Its contents should not be quoted or referred to in whole or in part without our prior written consent, except as required by law. Deloitte LLP will accept no responsibility to any third party, as the report has not been prepared, and is not intended for any other purpose.

Contents

Introduction and Executive Summary

As Internal Auditors, our role is to provide the Audit Committee, University Court and management with independent assurance as to the adequacy and effectiveness of the systems of internal control we review and to report weaknesses identified together with recommendations for improvement. We fulfil this role by performing appropriate audit work as agreed with the Audit Committee. Overall messages for the Audit Committee for the year ended 31 July 2009 are as follows:

- Our Internal Audit reports this year have identified 102 recommendations. This represents a reduction of 21% from 2007/08 when we raised 129 recommendations. 8 recommendations are rated Priority One, compared to 14 Priority One recommendations in the previous year. A summary of the Priority One recommendations is included on page 2. Overall our impression is that the control environment within the University continues to improve. While the overall number of recommendations has not reduced significantly, we believe this is more due to the Internal Audit coverage being expanded into areas not previously reviewed.
- Five out of eight Priority One recommendations relate to business and financial management within the Small Animal Hospital, the Weipers Centre for Equine Welfare and Hospitality Services. These are areas where pricing and financial structures and strategies were found to be insufficient and did not demonstrate value for money, but are not considered pervasive across the organisation.
- We have noted improvements in the core financial processes reviewed, specifically through our work in Purchase to Pay which identified wholesale changes to the controls over accounts payable through the introduction of the Purchase to Pay module on Agresso. Our additional work around the financial processes of insurance management and pension schemes identified no significant control weaknesses.
- The structure and management of Information Technology continues to be an area of relative weakness and our work on IT Resource Management has prompted further internal reviews of the approach to key elements of IT Services, including email, data storage and helpdesk facilities. Our follow up work has noted some progress in the implementation of outstanding recommendations, however the decentralised structure means this process is highly consultative and often time consuming.
- Over the year we have continued to support the development of risk management throughout the University. We have worked with representatives from the Faculties to further develop the template and processes for risk management, including clear identification of remediation actions. We also met with the Senior Management Group on 28th October to further encourage the embedding of best practice risk management.
- The results of our follow up on previous audit recommendations show that overall 43% of recommendations have now been fully implemented, 39% have been partially implemented and 18% have not yet been implemented. A number of the outstanding issues relate to the upgrading of systems within Finance and IT areas, which it is recognised will take longer to implement.
- Since the last Audit Committee meeting we have finalised our reports IT Network Security and Data Handling (see pages 6-8). The Data Handling report included one Priority One recommendation which has been discussed and agreed with management.
- Three reviews from the 2008/09 plan are not yet fully complete. These are Research Grants and Contracts, Estates Maintenance and Court Governance . Further details can be found on page 9.

Priority One Recommendations

The eight Priority One recommendations raised during 2008/09 are summarised as follows. All of these issues have been agreed with management and action plans put in place to address the recommendations. The Court Office and Finance Office regularly report to the Audit Committee on progress against outstanding recommendations, and Internal Audit will independently follow up on all outstanding recommendations during 2009/10.

Commercial Pricing	There is a gap in the level of pricing guidance and challenge provided across the University for commercial activities, outwith the established R&E project approval process.
	Our review of a sample of commercial contracts identified two in particular (Small Animal Hospital and Weipers Centre for Equine Welfare) where the pricing structure is not robust and the process for calculating prices (based on staff time and cost of consumables) is open to significant error or omission.
	For the SAH / Weipers Centre for Equine Welfare, over 100 items had a lower mark up rate than required as per policy. It is acknowledged that there is a requirement for different mark-up rates for different products. However, from this analysis, we noted that there is no consistency in the method of determining and applying these mark-up rate bandings for all product groups and no process to review and confirm the mark up of individual items.
Staff Performance and Development	The P&DR process is not formally connected to decisions on pay and promotion, although we recognise that discussions and negotiations have commenced around the strengthening of links between performance and pay for some staff, in particular professorial staff. University policies on pay awards for each group of staff should be reviewed to clearly define the links with performance as measured through the P&DR process. These should include links to performance for any enhanced pay and for promotion or regrading decisions
IT Resource Management	The current structure of IT support services has Faculty teams reporting to Faculty management with no link or reporting line to the Director of IT Services. This has resulted in inconsistent practices and inefficient resource allocation. In addition, there are two Faculties where the IT teams are devolved to Department level (three Departmental teams at each Faculty), and one further Faculty with additional IT staff located outwith the central Faculty team. These structures should be revised with a view to combining these.
Hospitality Services	There has been no stock management system in place for the last two years which has led to issues such as a lack of stock counts, no recording of waste and a lack of guidance around ordering procedures such as minimum/maximum reorder levels. New stock control software has now been purchased and this requires to be installed.
	There is no overall strategic plan in place to guide the Service in the next 3-5 years. In particular there is no financial strategy in place which defines the approach to target markets, pricing and costs, including the underlying assumptions, and is supported by market research and benchmarking analysis.
Data Handling	There are a number of policies that include aspects of data handling but no single, central data handling policy. There is a lack of compliance monitoring to ensure staff are treating data in a controlled manner. There is consequently a lack of understanding or assurance over data handling, for example what information is stored locally; whether data transmissions between systems and to third parties are secure; and the extent of action taken on non-compliance with policies.

Annual Internal Audit Report

Report to the Audit Committee

As Internal Auditors we are required to provide the Audit Committee with an Annual Internal Audit Report. The University Court and its management are responsible for ensuring that a system of control, financial and otherwise, is established and maintained. This is in order to carry on the operations of the University in an orderly and efficient manner, to ensure adherence to management policies, to safeguard the assets, and to secure, as far as possible, the completeness and accuracy of records. Our responsibility as internal auditors is to evaluate significant systems and associated internal controls and to report to the Audit Committee on the adequacy of such controls and systems. We cannot examine the whole system of controls, financial or otherwise, nor is Internal Audit a substitute for management's responsibility to maintain adequate systems of internal control over financial and operational systems.

In considering our assessment of the framework of controls we have taken the following into consideration:

- results of audits undertaken during the year;
- follow up action taken in respect of previous year's audit work;
- our perception of the extent of risk and control awareness amongst the staff and management of University of Glasgow.

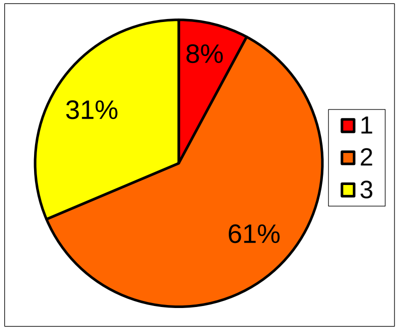
On the basis of work undertaken for the year ended 31 July 2009 we consider that University of Glasgow generally has an adequate framework of control over the systems we examined as summarised on page 4 (subject to implementation of the recommendations in particular those rated Priority One). In providing such an assessment we would draw to your attention our summary findings as presented in our individual reports issued throughout the year and particularly the Priority One recommendations.

We take responsibility for this report, which has been prepared on the basis of the limitations set out on page 12.

Overall Activity Summary

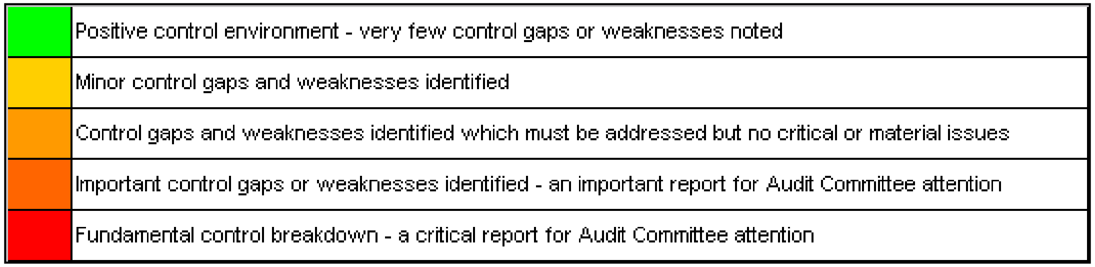
The following table provides a summary of the work we have undertaken in respect of the plan for 2008/09.

Project Title	Status / Timing	Budget (days)	Days to date	Recommendations		
2008/09				Priority 1	Priority 2	Priority 3
Review of Purchase to Pay (brought forward from 07/08)	Complete	15	15	-	5	1
Review of Commercial Pricing	Complete	25	27	3	6	1
Review of Pension Scheme Administration	Complete	10	10	-	-	-
Review of Corporate Communications	Complete	10	12	-	6	-
Review of Staff Performance and Development	Complete	15	17	1	3	1
Review of Sports and Recreation Services	Complete	15	15	-	3	3
Review of Student Services Relocation	Complete	20	20	-	5	2
Review of Insurance Management Arrangements	Complete	10	10	-	3	3
Review of IT Resource Management	Complete	20	23	1	3	2
Review of Programme Approval Procedures	Complete	15	16	-	4	2
Review of Hospitality Services	Complete	20	20	2	2	1
Review of E-Learning	Complete	15	16	-	2	4
Review of Faculty Corporate Planning	Complete	15	17	-	9	3
PAYE Compliance Risk Assessment	Complete	10	10	-	6	8
Review of IT Network Security	Complete	15	15	-	-	-
Review of Data Handling	Complete	15	15	1	5	1
Review of Estates Maintenance	Draft report issued	10	6			
Review of Research Grants and Contracts	Fieldwork complete	35	37			
Review of Court Governance	Fieldwork in progress	10	6			
Risk Management – Faculty Action Planning	Complete	15	15			
Whistleblowing Investigation	Complete	11	11			
Review of Student Lifecycle Workshops	Complete	15	15			
Audit Committee Effectiveness and TOR Review	Complete	7	7			
Risk Management – Risk Workshop	Complete	8	8			
Follow Up	Complete	20	20			
2008/09 Plan Development	Complete	10	11			
Contract Management Time	Complete	25	31			
Audit Committee	Complete	15	17			
		426	442	**8**	**62**	**32**



Project by Project Summary

A summary of the projects which have been undertaken since the last meeting is outlined on the following pages. Where applicable, the ‘temperature gauge’ is intended to provide Audit Committee members with a relative feel for the impact and overall importance of the findings of each project.



🟩	Positive control environment - very few control gaps or weaknesses noted
🟨	Minor control gaps and weaknesses identified
🟧	Control gaps and weaknesses identified which must be addressed but no critical or material issues
🟧	Important control gaps or weaknesses identified - an important report for Audit Committee attention
🟥	Fundamental control breakdown - a critical report for Audit Committee attention

Project by Project Summary

Review of Data Handling

🟩	🟨	🟧	X	🟥

Recent information security breaches by a number of publicly funded bodies have resulted in the Scottish Government actively seeking to improve data handling practices. Its main objective is to ensure that good data protection practices are implemented to prevent data leakages that could result in significant reputational damage and financial loss.

Data handling is the process of ensuring that manual and electronic data is stored, archived or disposed in a safe and secure manner during and after its use. This includes the development of policies and procedures to manage data and should consider the different types of data, various types of media and storage, responsibilities and privileges, and mechanisms for archive, retention and disposal. The purpose of this review was to conduct a high level assessment of the data handling methodology in place to evaluate the design of the controls and processes implemented.

Our overall conclusion was that significant work is required to reach a satisfactory level of control over data handling on a University-wide basis. A summary of our main recommendations and conclusions is as follows:

- There are a number of policies that include aspects of data handling but no single, central data handling policy. There is a lack of compliance monitoring to ensure staff are treating data in a controlled manner. There is consequently a lack of understanding or assurance over data handling, for example what information is stored locally and whether data transmissions between systems and to third parties are secure, and what action is taken on non-compliance with policies. This issue is graded Priority One due to the significant risks associated with loss of confidential data.
- Data handling specific training course are available and are included as part of the induction session for new staff joining the University. However, it has been estimated that only 20% of staff attend this session. There is currently no mandatory training session with regard to data handling and the associated risks.
- A formal data handling policy should be created which considers all aspects of data handling across the University and its external partners and is based on an initial risk assessment. This policy should formally define data handling boundaries and require different levels of rigour and security in the management of data depending on its sensitivity and risk classification. Clear policies and guidance material should be documented in relation to encryption within the University.
- Responsibility for data handling within the University of Glasgow should be clearly assigned to an appropriate member of University management.

These issues and recommendations have been discussed with management and we await full management responses demonstrating the actions to be undertaken along with timescales for completion.

Priority	CW	PI	Total
1	1	0	1
2	4	1	5
3	1	0	1

CW = Control Weakness

PI = Process Improvement

Project by Project Summary

Follow Up of 2007/08 Network Security Review

🟩 🟨 X 🟧 🟥

The purpose of this review was to conduct a full follow up review of the 2007/08 Network Security review which assessed the University's controls over network security infrastructure, systems and hardware. The following areas were selected for review:

- General Network Security – including the logical security provisions in place to protect the University's IT systems, the administration of information security and the monitoring of the security of the University's key systems.
- Security Policy and Procedures Review – the applicable network security policies and guidelines for systems.
- Network Software and Hardware – including the provisions in place to handle current and future threats to the continued availability of the University's key network and system resources. This also included current hardware and software versions and patching levels.
- Monitoring and Management – the use of monitoring and management tools and resultant security metrics in relation to network usage, abuse, availability, behavioural analysis and security threats.

The departments within the University have varying levels of autonomy with respect to information technology. In 2007/08, we made 11 recommendations and the status of implementation of the outstanding audit recommendations by grade is shown in the following table:

Priority	Fully Implemented	Partially Implemented	Not Implemented	Total
One	1	0	0	1
Two	0	7	1	8
Three	1	1	0	2
TOTAL	**2 (18%)**	**8 (73%)**	**1 (9%)**	**11 (100%)**

The Priority One recommendation relating to inappropriate administrator accounts has now been fully implemented. Supervisor access to the root account was previously accessible through a number of routes but this has now been restricted by IP address so only authorised individuals can make fundamental changes to the environment.

The recommendations which remain outstanding (all Priority Two) relate to:

- the implementation of appropriate password standards across all systems, although we note some progress within the Central ITS department;
- user administration policies and procedures, where user access reviews are not performed on a regular basis;
- regular review of audit logs and the results of security scans;
- the implementation of appropriate security policies;
- the implementation of fit for purpose change control processes;
- The introduction of robust anti virus processes throughout the University;
- performing regular risk assessments; and
- enhancing physical access controls to server rooms.

These results represent adequate progress by the central IT Services team, however further improvements to the IT Security controls are hindered by the decentralised nature of IT support services throughout the Faculties.

Project by Project Summary

Follow Up on Prior Recommendations

While the Audit Committee receive regular updates on the progress of outstanding recommendations from management throughout the year, Internal Audit continue to independently review this through an annual assessment of the implementation status by discussion with management, review of documentation and further sample testing where appropriate.

We concluded that out of 190 outstanding recommendations, 82 (43%) have been fully implemented. 74 (39%) have been partially implemented and 34 (18%) have not been progressed.

Priority	Implemented	Partially Implemented	Not Implemented	Total
1	9	18	4	31
2	52	47	22	121
3	21	9	8	38
Total	**82 (43%)**	**74 (39%)**	**34 (18%)**	**190 (100%)**

The four Priority One recommendations not implemented relate to:

- Quality and Completeness of Data in the Student Records System, dependent on the progression of the Student Lifecycle project;
- The development of Business Recovery Plans for Faculties and Departments;
- The implementation of a programme of Business Continuity Testing;
- The roll out of a suitable accounting package for the University Trust, to replace the spreadsheets currently in use.

The following table shows the outstanding recommendations per year and demonstrates a year on year reduction in the total number. Eight recommendations from 2005/06 and 31 from 2006/07 remain outstanding, although it should be noted that some of these refer to significant system developments and restructuring within the University.

Year	Implemented	Partially Implemented	Not Implemented	Total
2005/06	9	5	3	17
2006/07	13	20	11	44
2007/08	60	49	20	129
Total	**82 (43%)**	**74 (39%)**	**34 (18%)**	**190 (100%)**

Specific reviews where good progress has been made (over 80% of recommendations implemented) include Library Procurement, Heritage Asset Management, Strategic Performance Management, TRAC and Tendering.

Reviews with poor performance (less than 20% of recommendations implemented) include International Student Recruitment, Space Management and Business Continuity Management. These outstanding recommendations will continue to be monitored by management throughout the year and followed up by Internal Audit independently.

2008/09 Plan Completion

The 2008/09 plan was reviewed mid-year and two additional reviews added to replace others where the work was requested to be deferred. These are summarised as follows:

Review of Research Grants and Contracts
The RAE results for 2008 rated the majority of research at University of Glasgow as being world leading or internationally excellent. In 2007/08, the University was successfully awarded 1,084 research grants totalling £103.89m. To fulfil its strategic ambition within research, it is important that the University has robust procedures in place outlining how research grants applications are to be submitted, how research grant awards are to be approved, and how the conditions of these research grants will be adhered to.

Our approach to the review of Grants and Contracts included discussions with academic staff and administrators as well as staff from the Grants team, Contracts team and Research and Other Services team within Finance. We also carried out testing of grants and contracts files to ensure that relevant processes, policies and procedures were being adhered to, and assessed the overall design of the current process.

Our fieldwork is complete for this review and we are currently in the process of discussing findings and recommendations with management. This report is expected to be finalised by the next meeting of the Audit Committee.

Review of Court Governance
The fieldwork for our review of Court effectiveness and governance is underway. We have completed a desktop exercise to review the adequacy and completeness of key documentation and plan to meet with a sample of Court members over the next month to discuss Court effectiveness to enable us to gain a qualitative self assessment for the review. The output for this review will be similar to the Audit Committee assessment prepared earlier this year.

Additionally, a review of Estates Maintenance was included on the plan for 2008/09. The completion of fieldwork has been delayed due to the progression of HR modernisation within the Estates & Buildings Service. A draft report is now with management for comments.

Internal Audit Plan 2009/10

Our strategy for Internal Audit in 2009/10 was presented to the last meeting of the Audit Committee. Since then we have adapted the plan slightly to account for input of the Audit Committee members including the addition of a review of Endowments and a review of Estates Acquisition and Disposal. In order to accommodate the review of Estates Acquisition and Disposal, we have removed the planned review of Estates Refurbishment Projects.

The revised summary project plan for 2009/10 is shown below:

Area	%	DAYS	PROJECT	DAYS
Strategic Planning	5%	18	Review of International Marketing Strategy	18
Core Operations	17%	66	Review of NSS Results and Action Planning	15
			Review of Student Recruitment and Retention	15
			Review of Commercialisation	18
			Review of International Partnerships and Collaborations	18
Support Processes	20%	82	Review of Staff Recruitment and Appointment	12
			Review of Estates Acquisitions and Disposals	15
			Review of Contract Risk Management	15
			Review of IT User Administration	15
			Review of Carbon Reduction Management	10
			Review of Value for Money Indicators	15
Financial Management Processes	18%	70	Review of Fraud Management	18
			Review of Voluntary Severance Schemes and Payments	12
			Review of Sales Order Processing	15
			Review of Endowment Funds	10
			Review of Capital Asset Management	15
Risk and Regulatory Compliance	17%	70	Risk Management Workshop and Training	15
			Review of Health and Safety Governance	15
			Review of TRAC	15
			Review of Clinical Trials Management	10
			Review of EC Funding	15
Business Change	4%	15	Review of Student Lifecycle Project	15
Internal Audit Management	19%	79	Contract Management	25
			Audit Committee	18
			Contingency	18
			Follow Up	18
	100	400		400

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.

Deloitte LLP

Glasgow

October 2009

In this document references to Deloitte are references to Deloitte LLP.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom member firm of Deloitte Touche Tohmatsu ('DTT'), a Swiss Verein whose member firms are separate and independent legal entities. Neither DTT nor any of its member firms has any liability for each other's acts or omissions. Services are provided by member firms or their subsidiaries and not by DTT.

Deloitte.