

ISC11D025

University of East Anglia –Internal Audit Report

Student Records Application

March 2011

Draft for discussion purposes only

Distribution list:

Jonathan Colam-French

Jonathan Richardson

Audit Committee (Final report only)

Key dates:

Date of fieldwork: January 2011

Date of draft report: February 2011

Receipt of responses: xxx

Date of final report: xxx

This report has been prepared on the basis of the limitations set out in Appendix C.

This report and the work connected therewith are subject to the Terms and Conditions of the contract dated 12/07/10 between the University of East Anglia and Deloitte LLP. The report is produced solely for the use of the University of East Anglia. Therefore you should not, without our prior written consent, refer to or use our name or this document for any other purpose, disclose them or refer to them in any prospectus or other document, or make them available or communicate them to any other party. No other party is entitled to rely on our document for any purpose whatsoever and thus we accept no liability to any other party who is shown or gains access to this document.

Contents

1.	EXECUTIVE SUMMARY	1
2.	SCOPE OF ASSIGNMENT	2
3.	OBSERVATIONS AND RECOMMENDATIONS	4
	Recommendation 1: Project Team Responsibilities (Priority 3)	4
	Recommendation 2: Change Control Process Documentation (Priority 3)	5
	Recommendation 3: Greater Use of e-vision (Priority 4)	6
	APPENDIX A – REPORTING DEFINITIONS	7
	APPENDIX B – STAFF INTERVIEWED	9
	APPENDIX C - STATEMENT OF RESPONSIBILITY	10

1. Executive summary

1.1. Background

As part of the Internal Audit programme for 2010/11 we have undertaken an audit of the University of East Anglia's (the University) systems of internal control in relation to the Student Records Application.

The Application is used to administer the details of Students and related data.

1.2. Objectives and Scope

The overall objective of this audit was to evaluate and test the adequacy and effectiveness of the key controls over the Application in the following areas:

- Access controls;
- Data Input;
- Data Processing;
- Data Output;
- Interface Controls;
- System Auditing Features; and
- System Support and Change Control.

1.3. Summary assessment

Based on the work undertaken as detailed in the 'Objectives and Scope', our overall conclusion in respect of the adequacy and effectiveness of the controls over this application is **Substantial** assurance at the time of our fieldwork, subject to the exceptions raised and limited to the internal audit scope.

Full	Substantial	Limited	None
			

Substantial assurance is defined as, 'While there is a basically sound system of internal control, there are weaknesses, which put some of the system objectives at risk, or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk. '.

Our opinion reflects the state of the controls, including the control environment. The details of our report should be read in this context.

Management should be aware that our internal audit work was performed according to UK Government Internal Audit 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 an audit. The classifications of our audit assessments and priority ratings definitions for our recommendations are set out in more detail in Appendix A.

1.4. Key findings

The application has been in place since 2005, although the project team that managed the implementation remains in place providing ongoing application support and the resource to manage new functionality requests. It was felt that the project team's remit should not be as a support function and that those duties should be transferred over to another more suitable function.

The e-vision web front end was noted as being a much stronger tool than the SITS:Vision client in affording greater control over the data formatting and access management. There are a number of tasks that have already been implemented, although they form a very small proportion of the potential that could be mapped into the e-vision task mechanism. Given the access control weaknesses within the SITS:Vision client around being able to limit administrator access and tailor field validation, greater use of the e-vision system should be considered. It is acknowledged that there are resource challenges in this respect given the need to develop further functionality in-house.

There are documented change control processes in place to manage application updates, which involves user testing groups to provide User Acceptance Testing and Signoff evidence. Sample evidence to demonstrate these processes was not available for the audit, which has resulted in a recommendation being raised to ensure that adequate and documented change control processes are in place and filed for later reference.

As a result of our audit, we have not raised any priority 1 or priority 2 recommendations.

We have identified two priority 3 recommendations and one priority 4 recommendation.

Full details of the audit findings and recommendations are shown in Section 3 of this report.

1.5. Management Response

We will include a summary of the management responses in our Final report.

1.6. Acknowledgement

We would like to take this opportunity to thank all staff involved for their time and co-operation during the course of this visit.

2. Scope of assignment

2.1 Objective

The overall objective of this audit was to evaluate and test the adequacy and effectiveness of the key controls over the management of the Student Records Application.

2.2 Approach and methodology

The internal audit approach was to develop an assessment of risks and management controls operating within each area of the scope. The following procedures were adopted:

- discussions with management and staff at the University as necessary;
- identification of the role and objectives of each area of the scope and understanding the processes in place;
- identification of risks within the system;
- identification of existing controls within the system and assessment of the extent to which, if operating effectively, these mitigate the risks identified;
- testing of selected existing controls to gain evidence of their effectiveness on a judgemental sample test basis;
- discussion of findings with management; and
- raising and agreeing with management actions to improve control over the system.

2.3 Areas covered

In accordance with our agreed terms of reference dated 5th January 2011, our work was undertaken to cover the following system control objectives:

- Access controls;
- Data Input;
- Data Processing;
- Data Output;
- Interface Controls;
- System Auditing Features; and
- System Support and Change Control.

3. Observations and Recommendations

Recommendation 1: Project Team Responsibilities (Priority 3)

Recommendation

Management should review the scope of the project team to ensure that it is not providing ongoing support to existing functionality but focuses on the new functions that University management are specifying.

Observation

A review will help to ensure that project resource is assigned to project priorities rather than application support provision.

Although the application has been implemented since 2005, the project team that managed the implementation remains in place. This has partly been due to requests for new specifications being received and which need to be managed into the application but also because the project has also evolved into a support function that manages user account privileges and certain existing functionality like the timetabling feature.

There is an increased risk of inappropriate usage of available resource, which could affect both the support provided to the application and delivery of future project requirements.

Responsibility

Director of Information Services and SITS Project Board

Management response / deadline

Disagreed

Given limited resource levels we have deliberately taken the conscious decision not to separate new development from support. A plan of work is developed on annual basis, this plan draws together all of the requests for new development along with the known support requirements (upgrades etc.). The plan of work is prioritised by the SITS Project Board and resources allocated accordingly. We believe that this approach works well and do not agree with this recommendation.

We have identified that there may be opportunities for improvements to our more general project management approach and have engaged the SUMS Consulting to undertake a review of the methodology. This review may recommend some changes to the SITS project structures.

We are therefore happy to accept the low residual risk of non implementation.

Recommendation 2: Change Control Process Documentation (Priority 3)

Recommendation

Management should ensure that all change control processes and testing is documented adequately and filed for future reference.

Observation

Adequate documentation of the processes will help to demonstrate that change control processes are robust and complied with at all times.

Although there are documented change control processes in place for managing application updates and patches, there is no evidence retained to demonstrate those processes are operating as testing documentation could not be supplied for the audit. Hence, there is inadequate assurance as to the adequacy and effectiveness of those processes.

There is an increased risk of inadequate accountability for change control, which could result in a failure of the upgraded application.

Responsibility

Assistant CIS Director

Management response / deadline

Agreed

The unavailability of testing documentation for the audit was a consequence of various staff being absent on long term sickness and/or annual leave. It is accepted that a more transparent process for filing information needs to be developed in order that documentation is not stored on personal file store. Where paper documentation is stored there is a need to maintain a central register so that the location of relevant information can be identified.

CIS are in the process of implementing a change control process which will encapsulate the requirement to store and index change, testing and acceptance documentation. This is an ongoing project but will be in place for new changes/upgrades by September 2011.

Recommendation 3: Greater Use of e-vision (Priority 4)

Recommendation

Management should formally consider the use of e-vision capabilities to a greater extent.

Observation

More use of e-vision could help ensure greater control over data access and allow more devolved and controlled management of data entry and update.

The Student records application is a combination of the SITS:Vision client and e-vision web front end. The client's security model is weak in relation to configuring user access to specific data and screens, whereas tasks can be designed into e-vision that provide greater control of access to data and can also make completing tasks much simpler. The audit has noted that development of such tasks is very resource intensive and that the focus of the project team has to be on the more global system functionality requirements being asked of the application.

There is an increased risk of inappropriate or unauthorised data manipulation.

Responsibility

Director of Information Services / SITS Project Board

Management response / deadline

Agreed

The recommendation from auditor is welcomed and reflects our current strategy. We are well aware of the benefit of appropriate use of e-Vision and our strategy with SITS development is to e-Vision in preference to the client/server functionality however it is not always possible with complex processes to use e-Vision. We will consider each new development for e-Vision based on merit and cost/benefit received from the investment.

No further action required.

Appendix A – Reporting definitions

Audit assessment

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used:

Assurance Level	Symbol	Evaluation and Testing Conclusion
Full		There is a sound system of internal control designed to achieve the University's objectives. The control processes tested are being consistently applied.
Substantial		While there is a basically sound system of internal control, there are weaknesses, which put some of the University's objectives at risk. There is evidence that the level of non-compliance with some of the control processes may put some of the University's objectives at risk.
Limited		Weaknesses in the system of internal controls are such as to put the University's objectives at risk. The level of non-compliance puts the University's objectives at risk.
Nil		Control processes are generally weak leaving the processes /systems open to significant error or abuse. Significant non-compliance with basic control processes leaves the Processes/systems open to error or abuse.

The assessment gradings provided here 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' does not imply that there are no risks to the stated control objectives.

Grading of recommendations

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

Priority 1	Recommendations that are fundamental to the University, for the attention of senior management and the audit committee.
Priority 2	Recommendations that are fundamental to the area subject to internal audit, for the attention of senior management and the audit committee.
Priority 3	Recommendations that are important to the area subject to audit, to be addressed by management within that area.
Priority 4	Recommendations that are administrative issues, either from a best practice perspective or to address minor non compliance with existing control systems.

Appendix B – Staff interviewed

The following personnel were consulted:

Jonathan Colam-French	-	Director of Information Services
Jonathan Richardson	-	Assistant CIS Director
Emma Koro	-	Head of Application Support and Analysis
Helen McSparron	-	CIS Report Developer
Ian Callaghan	-	Head of the Planning Office, Academic Division
Garrick Fincham	-	Assistant Registrar, Academic Division
Julia Jones	-	Senior Administrator, Science Faculty Teaching Office
Ben Petley	-	SIS Application Specialist
Laura Thompson	-	Admissions Manager, Marketing and Admissions
Helen Roberts		Operations Officer, Marketing and Admissions

We would like to thank the staff involved for their co-operation during the audit.

Appendix C - 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

St Albans

March 2011

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

Registered office: Hill House, 1 Little New Street, London EC4A 3TR, United Kingdom. Registered in England and Wales No 4585162.

Deloitte & Touche Public Sector Internal Audit Limited is a subsidiary of Deloitte LLP, the United Kingdom member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, whose member firms are legally separate and independent entities. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Member of Deloitte Touche Tohmatsu Limited