ISC11D026
University of East Anglia –Internal Audit Report

IS Incident Management

July 2011

Draft for discussion purposes only

Distribution list:

Jonathan Colam-French, Director of Information Services

Michael McGarvie, Director of Faculty Administration, Faculty of Science

Andrea Blanchflower, Director of Faculty Administration, Faculty of Social Sciences

John Tully, Director of Faculty Administration, Faculty of Arts and Humanities

Helen Lewis, Director of Faculty Administration, Faculty of Health

Audit Committee (Final report only)

Key dates:

Date of fieldwork:	*May 2011*
Date of draft report:	*13 June 2011*
Receipt of responses:	
Date of final report:	

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

Contents

1. Executive summary

1.1. Background

As part of the Internal Audit programme for 2010/11 we have undertaken an assessment of the University of East Anglia's (the University) systems of internal control in relation to IS Incident Management. The Network Incident of December 2010 has been used as an example to illustrate the existing controls.

In December 2010, the University's Network Core suffered a major breakdown that resulted in IT disruption to varying extents across the university for approximately 56 hours. In addition, telecommunications were also affected, which hindered effective communication in the first hours following the outage. The timing of the disruption was also near to assignment deadlines and therefore a critical period for students and staff alike with reputational risk and potential for an increase in student complaints or appeals.

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 IS Incident Management in the following areas:

- Reporting information security events and weaknesses;
- Management of information security incidents and improvements;
- Responsibility and procedures including:
    - procedures for handling different types of security incidents, (loss of service or data by error or misuse);
    - analysis and identification of the cause of the incident;
    - containment;
    - planning and implementation of corrective action to prevent recurrence;
    - communication with those affected by or involved with recovery from the incident;
    - reporting the action to the appropriate authority; and
    - action to recover from security breaches.
- Learning from information security incidents; and
- Collection of evidence.

This scope is in line with the international IT Security Standard ISO27001 and as such is recognised as good practice. The scope provides a logical structure for the monitoring, identification, resolution and investigation of IT Security incidents. Although the Network outage was not a result of a security incident, the process itself could have aided in the monitoring, communication and recovery of the service.

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 IS Incident Management is **Limited** assurance at the time of our fieldwork, subject to the exceptions raised and limited to the internal audit scope.

Full	Substantial	Limited	None
			

Limited assurance is defined as, 'Weaknesses in the system of internal controls are such as to put the University's 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

ISD undertake retrospective reviews of relevant device logs should there be a need to do so. This was done on the occasion of the December outage. The review noted that the same error condition that caused the breakdown had also occurred to lesser extents on two previous occasions – August and October 2010. The multiple redundancy built into the devices ensured that the devices could recover from those instances, although this was not sufficient to prevent the December incident from happening. In addition, the error conditions were not familiar to ISD staff or the local support contractor, which resulted in a need to escalate the issue to the manufacturer, which contributed to the delays in recovery. Had there been a process whereby the logs are reviewed on a regular basis, the unknown error code may have been noted sooner and investigated as above before any serious issues were encountered.

ISD have no current forum for the discussion of technical, Information Security type issues that the department may be encountering. This has partly been due to the organisational structure of ISD senior management in that the Library Directorship is included with ISD. From August 2011, the University's integration project will result in a more technical structure being implemented, which will help to allow such a forum to be created.

The initial lack of telecommunications should be addressed by the use of alternative telecommunication means. For example, all relevant University Senior Management, especially within the Faculties, should be issued with Mobile Telephones or provide up to

date contact details, to allow them to be contacted should a similar event occur. This should form part of a wider Emergency Action Procedure that includes hard copy lists of relevant mobile and landline contact details stored on and off campus.

As a result of our audit, we have raised one priority 1 recommendation covering the use of log monitoring tools and subsequent proactive log monitoring.

We have identified two priority 2 recommendations, which are fundamental to the system and provide scope for improvements to be made. These are set out below:

- Recommendation 2: Information Security Forum;
- Recommendation 3: Emergency Action Procedures; and

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 IS Incident Management.

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 23rd April 2011, our work was undertaken to cover the following system control objectives:

- Reporting information security events and weaknesses;
- Management of information security incidents and improvements;

- Responsibility and procedures including:
    - procedures for handling different types of security incidents, (loss of service or data by error or misuse);
    - analysis and identification of the cause of the incident;
    - containment;
    - planning and implementation of corrective action to prevent recurrence;
    - communication with those affected by or involved with recovery from the incident;
    - reporting the action to the appropriate authority; and
    - action to recover from security breaches.
- Learning from information security incidents; and
- Collection of evidence.

3. Observations and Recommendations

Recommendation 1: Log Monitoring (Priority 1)

Recommendation

Management should implement a process of regular, documented log reviews and automated error notifications. Any priority findings should be investigated and action taken and reported to senior management as part of the IT Security forum noted in another recommendation in this report.

Where the manual review of logs is too onerous, automated tools should be used for collation of log information and analysis to identify trends and notify staff of potential issues.

Observation

Regular log reviews and automated error notifications will help to ensure that key events can be managed effectively and in a timely manner, potentially avoiding significant disruption or breaches of security.

ISD does not currently review its network device logs on a regular basis. However, logs are reviewed retrospectively should a particular event be deemed to require it as was the case for the December Network outage. The retrospective review noted that the error that caused the outage had also been logged in August and October 2010. Due to the fact that these events did not result in a network outage and because the logs are not reviewed, these occurrences were not noticed. Had a review process been in place, it is possible that the error event would have been noted, investigated and found to be something that required further work to resolve, which may have prevented the December failure.

The lack of logs reviewed and automated error notification, increases the risk that key events may be missed, which could result in the eventual degradation or failure of the IT service.

Responsibility

ICT Systems Director

Management response / deadline

Agreed in principle

Our network equipment supplier does not inform customers of fault code descriptions and significance and we would require this information to review the logs in any meaningful way. It should also be noted that over a six month period the log files are likely to contain in excess of twenty five million records ruling out any manual review.

We have a support contract with the suppliers who use the log files as the initial point of investigation for equipment failures and due to the volume of data it is only practical for them to focus on the incident timeframe. The investigation by our supplier into the December network outage allowed them to identify a particular error code as significant, allowing them to look for previous incidences. Prior to this investigation the significance of this error code was not known ruling out the value of a regular log review to this particular incident.

Development of automated in-house log review code is something we would not consider due to the high risk of the supplier changing the log format and them adding or discovering the significance of new codes, without informing us. We will contact our supplier to request that an automated and proactive log review is a something they should consider developing as a service for key customers. Assuming this is something

they are willing to develop we will review the cost of this service against the likelihood of any future occurrences; the cost of this is likely to be significant and the business benefit needs to be considered by ISSC.

Audit Comment:

Should the costs of an automated service provided by the supplier prove prohibitive, or the supplier chooses not to develop automated monitoring then ISD should prepare a paper for the Audit Committee to identify any next steps.

Recommendation 2: Information Security Forum (Priority 2)

Recommendation

IT Management should create an IT Security forum that meets periodically to discuss current IT Security issues that may affect its service. Inputs into the forum could include the following, although the list should not be considered to be exhaustive:

- Summary data regarding possible hacking attempts;
- Summary data regarding key security issues noted in the wider Higher Education community;
- Reporting on phishing attempts and numbers of intercepted/blocked emails; and
- Reports on IT service events that require management review and action, with possible key log events being presented as part of the reporting.

The meetings should be documented and actions arising regularly reviewed.

Observation

Regular meetings will help to ensure that relevant issues are raised, discussed and managed appropriately.

There is no current forum for the discussion of IT Security, although there is an ICT forum which is largely used to advise senior University management on IT policy issues.

The lack of relevant forums increases the risk that relevant issues are not raised and managed effectively, which could result in errors and service degradation.

Responsibility

Director of Information Services

Management response / deadline

Agreed / October 2011

We do not agree with the assertion that IT security is not discussed. ICT security issues are discussed within the CIS and ICT Heads meetings; they are discussed at ISD management team meetings and if appropriate at the wider ISD Heads meetings. The ICT Security Project provides a further forum for this discussion and as part of this project we are discussing departmental ICT security matters directly with Heads of School. The ICT security project has been recognised as being of vital importance at UEA and is a standing item for report and discussion by ISSC.

The Administrative Integration Project transfers line management responsibility for local IT support staff to ISD and in order to embed these new structures an alternative approach will be required to team meetings to ensure cross divisional join up. As part of the new structures we plan to create an IT Problem Management Group, this group will comprise staff from 1st, 2nd and 3rd line support functions, one of the remits for this group will be to review information on ICT security matters. This group will be in place from September 2011.

Recommendation 3: Emergency Action Procedures (Priority 2)

Recommendation

University Senior Management should draft and agree processes and procedures that guide the management of incidents such as the IT outage in December 2010. The process needs to be consistent, communicated to all relevant University staff and comprise the following elements as a minimum:

- A current contact list of key staff, including mobile/home numbers. This may require key listed staff to be provided with mobile telephones for work purposes;
- A Draft meeting agenda to avoid the need to draft one when an event occurs;
- An escalation procedure that describes the roles and responsibilities of key staff for such events. For example, who has the responsibility to call relevant staff to emergency meetings;
- Processes around the effective, timely and consistent communication of events via relevant media services, for example social networks and press releases; and
- Formal documentation of all meetings, communicated to all attendees and other relevant senior management for reference.

Copies of the agreed procedures should be kept in hard copy and held onsite and offsite in locations known to all relevant personnel for ease of reference. Processes should also be subject to regular review to ensure that they remain current to possible changes to University requirements.

Observation

Agreed processes held offsite in hard copy will help to ensure consistent and effective management of such events.

The events in December meant that the intranet could not be consulted for staff telephone numbers, nor could the telephones themselves be used effectively as they were also largely affected by the event, being connected to the network. This resulted in the need to physically locate relevant staff in their offices, with the possibility that they would not be there. One of the Faculty Administration Directors could not be contacted to advise them of the initial emergency senior management meeting called by the Registrar.

The lack of agreed, formal processes increases the risk of ineffective management of such incidents.

Responsibility - VCO

Management response / deadline

Agreed / October 2011

The Vice-Chancellor's Office is in the process of revising and up-dating the University's business continuity plan to bring it into line with the newly integrated administrative structures. It is intended that from 2011, the emergency contact sheets will duplicate the call-out register held by UEA Security.

The current plan contains emergency contacts for a core group of staff and reference sheets for contacts in the event of emergencies involving key services such as accommodation and scientific laboratories, and other emergencies such as pandemic flu or meningitis. There is a communication protocol within the Plan which will be revised and up-dated as part of this process.

Meetings of the Registrar's core team for such emergencies are administered by staff in the VCO suite and notes kept and circulated as appropriate to the nature of the crisis.

Copies of the current plan are held on-site and off-site and it is intended that this will continue to be the case.

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
Peter Andrews	-	Head of Networking
Iain Reeman	-	ICT Systems Director
Michael McGarvie	-	Director of Faculty Administration, Faculty of Science
Andrea Blanchflower	-	Director of Faculty Administration, Faculty of Social Sciences
John Tully	-	Director of Faculty Administration, Faculty of Arts and Humanities
Helen Lewis	-	Director of Faculty Administration, Faculty of Health

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

July 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.