I. Background

Industry Story

The Problem with Unmanaged End User Computing Applications

Researches revealed that about 68% of an enterprise’s corporate data is stored in applications managed and controlled by IT department. The other 32% of corporate data is stored in Microsoft Excel spreadsheets, other databases (e.g. Microsoft Access), business intelligence tools (e.g., reporting tools), Microsoft Word documents, web-oriented architecture “mashup” approaches and other end user computing applications. Often the 32% portion of corporate data exists in relatively uncontrolled environments and may lack the same safeguards and controls applied to the 68% portion of corporate data under the IT Department control.

Such deficiency in safeguards and controls can result in negligent errors, as was the case with TransAlta Corp., which took a $24 million charge to earnings after a bidding error caused by a cut-and-paste mistake in an Excel spreadsheet. The lack of adequate safeguards and controls can also permit dishonest users to engage in fraud, as happened with AIB’s Allfirst Bank, where a trader hid a $700 million loss by substituting links in a company spreadsheet to his private manipulated spreadsheet. For regulated enterprises, this can lead to regulatory compliance issues.

See the article: (http://blogs.msdn.com/b/grc/archive/2009/07/01/the-problem-with-unmanaged-end-user-computing-applications.aspx)

End User Computing Overview

End User Computing (“EUC”), also known as User Developed Applications (“UDA”) is a popular approach that involves end users with non-programming knowledge in design, creation and maintenance of working applications. Unlike conventional program development, assembling EUC programs is performed at application level of existing software packages. For examples, formulae entered in Microsoft Excel spreadsheet, analysis programs made by Statistical Analysis System (“SAS”) and macros embedded in Microsoft Word.

From end users’ perspective, the use of EUC is convenient and efficient, as it can be created and maintained locally. However, when talking about information security, EUC has a new set of problems, including weak access control, uncontrolled change process, higher possibilities of mistakes and loss of data. Poor management of EUC could eventually lead to exploitations on those security vulnerabilities.
II. Management

EUC programs that store and manipulate important information (e.g. financial figures, examination records, research data) of universities should be subject to same level of general IT controls implemented on applications controlled by IT department. Nevertheless, since the IT departments do not own those EUC programs, the first step towards effective EUC management is establishing a EUC control policy, covering the following elements:

Definition

Each academic or administrative unit may have different interpretations of EUC applications, which may result in obstacles during the implementation of EUC controls. Management should provide clear definition of EUC programs and communicate to universities’ staff, students and any relevant members.

EUC Register

A EUC register should be created by each academic or administrative unit to record all existing EUC programs. The nature of EUC programs should be identified and categorised into corresponding classes (e.g. financial, academic, operational, and informational). In addition, the ownership, including the owner’s name and respective academic or administrative unit, of each EUC program in the register should be documented. Management should also ensure that the EUC register is regularly updated to avoid any incorrect information kept within.

Risk Assessment

The risk assessment process evaluates the risk level of each EUC programs in the EUC register based on its nature and the classification of information (e.g. confidential, internal and public) it stores/manipulates, considering the following risks due EUC errors or frauds:

- **Financial Risk** – Financial misstatement
- **Academic Risk** – Incorrect research conclusions of findings
- **Operational Risk** – Impact or interruption to operations
- **Informational Risk** – Misleading information

Based on the risk assessments results (e.g. high, medium low), adequate level of security controls can be deployed for EUC programs, which helps to better utilise the limited resources for EUC management. The risk assessments should be performed at least once each year to ascertain the validity of assigned risk levels and maintain the appropriateness of the controls implemented over EUC programs.

References:
II. Management (Cont’d)

Control Requirement

Based on the classes and risk levels of EUC programs, the minimum requirements on EUC controls can be determined. Similar to IT general controls, typical EUC controls come from the following four areas:

- **Access Control**: Logical or physical controls determine who can access specific EUC programs and what is the authorisation procedure required. For high risk EUC programs, the number of authorised personnel should be restricted to minimum. Granting access to EUC programs are usually done by the EUC owners. Documented evidence on access authorisations should be retained for further reference or investigation purpose.

- **Change Management (Version Control)**

  Changes to existing EUC programs are made in a controlled manner. The owners of EUC programs should review the change requests. High risk EUC program changes may also require the endorsement from the senior management. Before officially using the changed EUC programs, independent testing of changed EUC programs should be performed to ensure there are no mistakes, such as miscalculation and program errors. Documentations related to change requests (e.g. e-mails, request forms) and testing (e.g. test case, test result) should be maintained for each version of EUC program.

- **EUC Development**

  Controls over EUC development are similar to those implemented for EUC changes. It is EUC owners’ responsibilities to ensure that all new EUC programs are developed with their consent and properly tested before being officially used by end users.

- **Operations**

  Backup, restoration and problem management are the key components of EUC operations controls. Management may take a centralised approach (i.e. performing backup, restoration and problem management for EUC programs centrally by IT department) or execute the operations controls in a distributed way (i.e. each academic or administrative unit back up, restore and provide troubleshooting services for its own EUC programs).

**Monitoring**

Periodic review or internal audit on the relevant controls over EUC programs are recommended to be performed by universities. The purpose of doing this is to assess the effectiveness of EUC management adopted by the universities and detect any deficiencies (e.g. deviation from established control requirement, missing control area, etc.). Management should review the identified deficiencies, coordinate with corresponding EUC owners to work out the remediation plan and track the remediation process.
III. General Users

Best Practice to be Followed by General Users

To use EUC programs safely and effectively, the general users are recommended to follow the practice below:

- **Familiarise with EUC Policy** – The very first step for using EUC programs is to familiarise with the EUC control policy. Users must be able to know what is a EUC program, who is the owner, what is the procedure to change the EUC program, and whom should be contacted if the EUC program is accidently deleted / modified.

- **Avoid Unauthorized Access** – Users are recommended to utilise the security functions that come along with the software packages. For example, password protection features in Microsoft Excel spreadsheets. The passwords should not be disclosed to unauthorised parties and should be changed regularly.

- **Avoid Mistakes** – When using EUC programs, it is important to use the correct versions before storing or processing the data. Wherever possible, manual reconciliation/verification on EUC program output should be performed. If the mistakes are related to EUC programs instead of manual errors, corresponding EUC problem management procedure should be followed by users. In addition, users should consider incorporating input validation controls when developing or updating the EUC programs to reduce to the possibilities of having incorrect results.

Conclusion

The convenience and flexibility of EUC has made it one of the most important IT components in universities’ computing environment. Good management of EUC allows universities to maximise the benefits of EUC and avoid the damage or loss caused by its vulnerabilities. General users can also increase their efficiency through the correct use of EUC programs and consistently following the EUC policy.

Copyright Statement

All material in this document is, unless otherwise stated, the property of the Joint Universities Computer Centre (“JUCC”). Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, without the prior written consent of the copyright holder, is a violation of copyright law.

A single copy of the materials available through this document may be made, solely for personal, noncommercial use. Individuals must preserve any copyright or other notices contained in or associated with them. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the copyright holder of the materials. Contact information for requests for permission to reproduce or distribute materials available through this document are listed below:

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC),
Room 223, Run Run Shaw Building,
c/o Computer Centre, The University of Hong Kong,
Pokfulam Road, Hong Kong

References:
http://www.isacapgh.org/07%20Event%20Archive/February_ISACA_Presentation.pdf
http://endusercomputing.org/category/best-practices/