WHEN END USERS CREATE TECHNOLOGY

Robert Newsome

9/21/2016
Agenda

• What are EUC (End User Computing) & EUCA (End User Computing Applications)
• Organizational Challenges
• Audit Challenges
• Complexities
• Solutions
What is End User Computing?
End-user computing (EUC) and End-User Computing Applications (EUCAs) refers to systems & applications in which non-programmers can create working applications outside a recognized formal IT areas.

End-user computing can range in complexity from users simply clicking a series of buttons, to writing scripts in a controlled scripting language, to being able to modify and execute code directly.
EUC Typical Example

• Typically Microsoft Office Products like Spreadsheets (MS Excel) and Local Databases (MS Access)

• Business Intelligence reports (e.g. SQL Server analysis, Hyperion, Crystal Reports)

• New users are more and more IT literate and they deploy more computing power like reporting and scripting tools
Who uses them?

• Financial and business analyst can create spreadsheets to analyze and graph discrepancies between budget and actual performance numbers

• A back office employee uses a reconciliation file which compares records from one system to the GL

• Project manager can develop small DB to track progress of projects and employee assignments
How Common is it?

• In 2003, the Hacket Group (www.thehacketgroup.com) surveyed mid-size companies. It found that 47% of companies use stand-alone spreadsheets for planning and budgeting.

• In a webcast for Deloitte on May 22, 2005, the first author was able to ask a series of questions of the audience. The average response size was just over 800 financial professionals and officers in corporations. One question specifically asked, "Does your firm use spreadsheets of material importance in financial reporting?" Of the respondents, 87.7% answered in affirmative., while 7.1% said, "No." (Another 5.2% chose "Not Applicable.")

• In Europe, A.R.C. Morgan interviewed 376 individuals responsible for overseeing SOX compliance in multinationals that do business in the United States [TMCnet.com]. These respondents came from 21 different countries. More than 80% of the respondents said that their firms use spreadsheets for both managing the control environment and financial reporting.
Why we use them?

- Reduce Cost – Large ERP systems cost time and money to develop simple reports that users and management want
- Increase efficiency and less effort when doing repetitive task like looking for errors
- Less turn around time to make a change and see results in reports
Where are they used?

- Practically everywhere
- Back office departments, production plants, sales departments, IT shops, Various operations and Internal audit departments.
- Millions of managers and employees acting as end-user programmers design, build and use EUCA’s everyday
What can go wrong?

Bernard Lawrence "Bernie" Madoff, the former Chairman of the NASDAQ stock exchange and the admitted operator of the Ponzi scheme made "the largest investment fraud in Wall Street history". Madoff or DiPascali would enter trades that never happened, with real prices, into an old IBM AS/400 computer he used for his advisory business and – voilà! – he had a track record. Then, using a simple spreadsheet such as Excel, more than 2,300 client accounts were updated automatically – dividing among all the accounts the gains from the “trades” that amounted to “profits” of 1%. (Information Week Aug 2009)

Best Quote: “the obscurity of the AS/400 was critical in helping Madoff to conceal the scheme for such a long time.”
Another Example

A rogue trader cost France’s Société Générale € 4.9 billion. Kerviel was able to circumvent SG's internal warning systems by opening and manipulating Excel spreadsheet reports used by managers to monitor traders' activities. (Business Ethics: Case Studies)

Best Quote of the article: "A common bad technique is to embed usernames and passwords into applications, especially Excel report sheets. These tend to be powerful administrator or developer accounts, granting unlimited access with little or no auditing."
Current State

• Most organizations are aware of the risks associated with the use of EUC’s (often documented during audits as the “key Spreadsheets”) usage and have made attempts to implement policies and procedures to control the usage of these EUC’s.
Organizational Challenges Today

– Governance
– People
– Process
– Technology
EUC Control Environment - Governance

• Definition and identification of EUCs
  – The definition generally distinguishes EUCs from IT-developed and supported applications and will determine which EUCs should be placed under management.
  – As part of the identification, decision criteria should be carefully defined for the organization. For example, are all Microsoft Access databases considered to be EUCs? All spreadsheets? Or only those that directly impact financial statements?
EUC Control Environment - Governance

• Policies and standards
  – Policies and standards establish a consistent framework for the control of the EUC environment in a company. They define criticality criteria, inventory standards, risk ranking, and control requirements of EUCs. Defined policies and standards will help ensure compliance and will provide a structure for auditing and monitoring.
EUC Control Environment - Governance

• Ownership
  – Defines the governance model for establishing an effective, sustainable EUC management program. There are three primary options: centralized governance throughout a project management office, decentralized governance with champions in each business unit, or a hybrid approach that combines aspects of each.
EUC Control Environment - Governance

• Monitoring and reporting
  – Key tasks include identification, tracking, and reporting metrics associated with all phases of the EUC management program to key stakeholders and senior management.
EUC Control Environment – People

• Roles and Responsibilities – Identify the key stakeholders
  – Once the key stakeholders are identified, the next step is to establish the roles and responsibilities of various stakeholders within the EUC management program. Stakeholder roles include the program sponsor, central program group, steering committee, business unit representatives, EUC users, internal audit, etc.

• Develop a training program to target each stakeholders group identified above.
  – The training will be targeted to different tiers of the EUC management program. Examples of the training include EUC policies implementation, EUC risks and controls steps, controls tool training involving end users and administrators, etc.
EUC Control Environment – Process

• Risk Ranking and Prioritization
  – Define the risk ranking model to determine the impact and likelihood of failure-related EUCs. A combination of qualitative (e.g., compliance and operational materiality) and quantitative approaches (e.g., financial materiality) can be utilized to create a risk ranking model.
  – Once the risk ranking model is defined, the model should be applied to identified EUCs to determine which should be placed under management. Clear definition of risk categories is important. Examples of possible risk categories could be:
    • High, medium, or low model
    • "In or out" model where high-risk EUCs are required to comply with all EUC controls, and low-risk EUCs are not required to comply with any EUC controls
EUC Control Environment – Process

• Inventory
  – Define an inventory approach
    • A specific strategy should be defined to determine how the inventorying process will occur, as well as decisions made about manual vs. automated approaches, use of surveys, rollout by business unit vs. geography, etc.
  – Create and maintain a central repository to maintain data
    • Implement a process to create and maintain an up-to-date inventory of business-critical EUCs. The central repository of EUCs contains critical information or metadata about the EUCs. Examples include risk ranking, description of EUCs, business owner and end-user information, business unit, etc.
  – Technical support requirements
    • To help ensure completeness, the organization has the option of using various automated tools to gather EUC Inventory.
EUC Control Environment – Process

• EUC Controls
  – Version control – helps ensure that the latest and approved version of EUC is used.
  – Change control – helps ensure that the changes to EUCs are appropriately tracked and reviewed.
  – Data integrity control – helps ensure data integrity.
  – Access control – helps ensure that only authorized users can access EUCs and in what manner (e.g., view, change, delete).
  – Availability control – helps ensure that EUCs are available in the event of disaster, accidental deletion, etc.
EUC Control Environment – Process

• Template
  – A template is an organizationally accepted guide after which all EUCs entered into the program are modeled. The templates provide consistency, conformity, and standardization of EUCs that are created, as well as documentation with respect to that individual EUC

• Baselining
  – The purpose is to help ensure that the EUC is functioning in accordance with management's intention in a point in time. Baselining involves validating the structures, formulas, calculations, inputs, and outputs of the EUC. Enrolling EUCs that have not been baselined into the EUC management program will provide less assurance that errors will not occur on a go-forward basis.
EUC Control Environment – Process

• Monitoring
  – To help ensure compliance with the EUC program, a process should be established to perform periodic testing so that EUCs enrolled in the program remain compliant and critical EUCs not under management become enrolled in the program. Testing will also help to ensure that the effectiveness of the EUC program does not degrade over time.
EUC Control Environment – Process

• Technical Assessment
  – Technology enabler requirements should be defined, and then available options such as manual processes vs. automated tools should be evaluated against the specific technical requirements. Vendor demonstrations and/or pilots should be performed. The current IT infrastructure should also be considered. (E.g., is there an existing Microsoft SharePoint deployment that can be leveraged?)

• Sizing and infrastructure
  – Determine key architecture decisions in the implementation. This may be contingent on strategic decisions made. For example, if network file shares will be used to secure EUCs, does the current server population have the estimated capacity to accept the additional load? Other considerations may impact this as well
EUC Control Environment – Process

• Security role design
  – One key control element that should be implemented is the restriction of access to EUCs. Different technical solutions provide different levels of assurance in this regard. For example, using network shares to secure EUCs will only protect access to the EUC file itself, while using a vendor tool may allow for controlling different types of access within an EUC, such as read access vs. change access. The organization will need to develop a detailed security roles design for controlling access (e.g., end users, reviewers, administrators), and then will need to configure the technology enablers accordingly. Processes will need to be established to maintain and administer security on an ongoing basis.

• Rollout strategy
  – EUC management is not a trivial undertaking. Many organizations struggle with trying to do too much too quickly. A deliberate rollout strategy should be defined that determines which business units, or regions, and which EUCs (high risk, medium risk, etc.) will be placed under management, and in what order. Data privacy requirements must be considered to help ensure compliance with laws and regulations, client requirements, etc.
Table Discussion Exercise

• Take 5 minutes and at each table discuss where your organization is at regarding the usage of EUCs
Audit Challenges

AUDITING

What my friends think I do
What my mom thinks I do
What society thinks I do
What the partners think I do
What I think I do
What I actually do
# Audit Methodology

<table>
<thead>
<tr>
<th>Standard ITGC Method</th>
<th>EUC Focused Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Security &amp; Data Integrity of items</td>
</tr>
<tr>
<td>User Access</td>
<td>User Access &amp; Segregation of Duties</td>
</tr>
<tr>
<td>Change Management</td>
<td>Input, Logic, Output Review &amp; Approval</td>
</tr>
<tr>
<td>Backup and Recovery</td>
<td>Backup</td>
</tr>
<tr>
<td>3rd Party Service Contracts</td>
<td>Documentation</td>
</tr>
<tr>
<td>Data Center</td>
<td></td>
</tr>
</tbody>
</table>
Example of Existing Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUCA Policy &amp; Control Standards</td>
<td>Define the responsibilities and processes surrounding EUCAs with the aim of placing responsibility for the risks arising and understanding and reducing these risks through inventory and mitigation processes.</td>
</tr>
<tr>
<td>Access Controls</td>
<td>Define and Restrict user access, rights and privileges</td>
</tr>
<tr>
<td>Change Controls</td>
<td>Define the process to be followed whenever specific types of changes are performed</td>
</tr>
<tr>
<td>Version Controls</td>
<td>Ensure accurate identification of the current production files</td>
</tr>
<tr>
<td>Development Controls</td>
<td>Control development, testing and approval of new critical EUCAs prior to deployment into production</td>
</tr>
<tr>
<td>Documentation</td>
<td>Require that EUCAs are adequately documented with regard to their use and design</td>
</tr>
<tr>
<td>Input Controls</td>
<td>Employment of data validation to control or restrict input to valid data.</td>
</tr>
<tr>
<td>Data Security and Integrity.</td>
<td>Balancing input data with totals form data sources.</td>
</tr>
<tr>
<td>Output Controls</td>
<td>Use of cross checks, balancing to ensure all input data has been accounted for and reflected in the outputs and to prevent or highlight potential calculation errors.</td>
</tr>
<tr>
<td>Segregation of Duties</td>
<td>Define duties, roles and responsibilities regarding the usage of EUCAs and design changes.</td>
</tr>
<tr>
<td>Backup and Archival</td>
<td>EUCAs should be maintained on a secured server that is backed – up on a regular basis. Prior versions of critical files should be moved to a secure archive folder to prevent data corruption and ensure they are not accessed or used in error.</td>
</tr>
</tbody>
</table>
Auditor Training?

• How do we successfully train auditors to ask the right questions when?
  
  • The majority of process or IT walkthroughs never mention the “EUC” applications that are in use or show databases listed within the process or data flows.
  • Data is now being shared from enterprise applications to Access databases with the support of IT.
  • Auditors may not have IT skills to determine risk or controls of newer applications.
Complexity issues?
Complexity Example

• Most Common EUCAs are spreadsheet applications
• End user databases like MS Access are the new trend
• New users are more IT literate
• File can be stored anyway – Locally, share drive, Share Points, USB drive, Web.
Database Complexity Example

• Complexity criteria for a simple local databases based on PWC Best Practices

• Auditor should evaluate
  – Number of tables
  – Number of Queries
  – Number of Forms
  – Number of Modules
Spreadsheet Complexity Example

• Complexity criteria for spreadsheet based on PWC Best Practices

• Auditor should evaluate
  – # of Sheets
  – Formules
  – Formules with errors
  – Array Formules
  – Nested Ifs
  – Max Nested Ifs
  – External Links
  – Macros
  – Pivot Tables
  – Names Items
  – Invisible Cells
  – Hidden rows and columns
  – Hidden sheets
  – workbook size
  – External Links
  – Macros
Other Challenges for Audit

- **Business Managed Technology** is a term to describe information-technology systems and solutions built and used inside organizations with the help of IT but managed by the business vs the traditional IT depts.

- Usually analytical type applications but growing into full fledge IT departments.
  - Local support and contact with vendors, suppliers and
  - Ability to be flexible and make changes now
  - Full Access to data and configurations

“Best practice would be a policy that clarifies that all technology at your organization is subject to your company’s IT standards, even where a component of technology is managed within a business and not in a CIO Council member’s organization”
Other Challenges for Audit Con’t

• **Shadow IT** is a term often used to describe information-technology systems and solutions built and used inside organizations without explicit organizational approval.
Where do we go from here?

- If starting from zero, begin with Google and search for The use of Spreadsheets by PriceWaterhouseCoopers. This report lists a large number of controls. The first step is to inventory all of a firm's spreadsheets that are "in scope," that is, are used in financial reporting. Next steps are to evaluate the riskiness of these spreadsheets, determine necessary controls, evaluate the existing (as-is) controls on these spreadsheets, and develop action plans for remediating control deficiencies.
It lists nine factors to consider when evaluating the "risk and significance" of a spreadsheet:

- Complexity of the spreadsheet and calculations
- Purpose and use of the spreadsheet
- Number of spreadsheet users
- Type of potential input, logic, and interface errors
- Size of the spreadsheet
- Degree of understanding and documentation of the spreadsheet requirements by the developer
- Uses of the spreadsheet's output
- Frequency and extent of changes and modifications to the spreadsheet
- Development, developer (and training) and testing of the spreadsheet before it is utilized
The report also lists a number of controls that should be considered to mitigate risks inherent in the spreadsheet environment.

- **Change control**: the authorization of change requests, testing the spreadsheet, and formal sign-off by another individual.
- **Version control**: Ensuring that only the current and approved version of each spreadsheet is used. Naming conventions that include version numbers and dates and the use of structured directories can help in this.
- **Access control**: assign appropriate access rights to people who need to use the spreadsheet. Use a password to control access.
- **Input**: Whether manual or automatic data entry is used, there should be reconciliations.
- **Security and data integrity**: storing spreadsheets in protected directories, and locking formula cells to prevent logic changes.
- **Documentation**: Ensure that the business objective and functions of the spreadsheets are understandable.
- **Development life cycle**: Use a standard systems development life cycle. The report specifically says that testing is critical (but does not discuss how to do testing).
- **Backup and Archiving**: spreadsheets should be backed up because of their sensitivity. They should be archived in read-only format for later review.
- **Logic inspection by an independent person other than the developer**: The report does not discuss how logic inspection is different from testing. Probably, testing is taken as what we call execution testing later in this paper. The report appears to sanction logic checking by a single individual. As discussed later, this appears to be unwise.
- **Segregation of duties/roles, and procedures**: There should be authorities, roles, and procedures for ownership, sign-off, and other matters. This item is so brief in the report that it provides little guidance.
Additional Resource: Global Technology Audit Guide (GTAG) 14: Auditing User-developed Applications – Via IIA website
QUESTIONS?