

## Controlling End-User Computing : Putting the Genie back in the Bottle

Ray Butler, CISA, FIRM

### Ray Butler...

- IS Auditor in HM Customs & Excise for 25 years
- Trained Tax inspectors in Spreadsheet Audit
- Co-Founder of European Spreadsheet Risk Interest Group
- Past President of ISACA Northern England
- Was Risk Manager ...
- ....Now Information Governance Lead for Highways Agency

## CYA Disclaimer

- I speak in a personal capacity
- All views expressed are my own...
- And don't necessarily reflect those of HM Government

## Today's agenda

- Commonest end-user applications and the risks involved in their use
- Impacts of material error in the use of end-user applications
- A CobiT- based maturity model to measure the likelihood of material error from use of end-user applications
- Identify some good and not so good practices in end-user applications
- Describe some options for improving control of end-user applications.

## What is end-user computing?

- Definition from Webopedia
  - Using a computer at the application level. The term end-user is used to distinguish the person for whom the product was designed from the person who programs, services, or installs the product. Developers working on a personal computer in a professional capacity, for example, are not considered end-users.
- Wikipedia
  - End User Computing (EUC) is a group of approaches to computing that aim at better integrating end users into the computing environment or that attempt to realize the potential for high-end computing to perform in a trustworthy manner in problem solving of the highest order. [1] [2] [3]

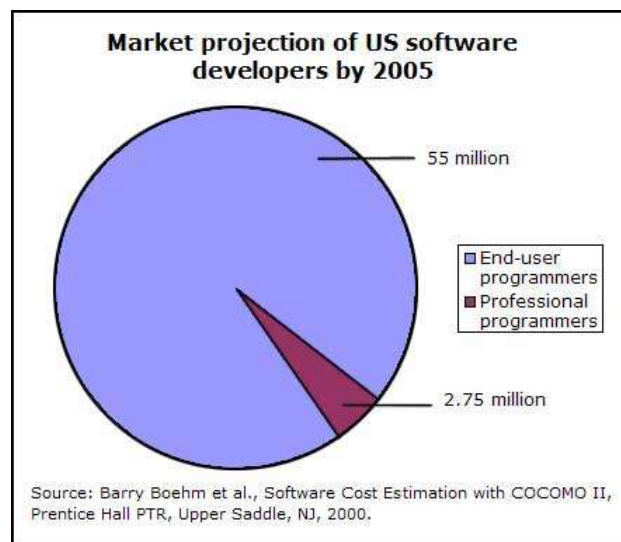
## Our texts for today...

- The Problem with end-user computing Is that end-users do it (anon)
- Q What is The Most dangerous component of a car?
- A The nut behind the wheel (Christmas Cracker Joke)

## A Request to Microsoft



## From the EUSES consortium



## Common Tools

- Spreadsheets
- Databases
- Word Processing
- Presentation Software
- e-mail
- Report Generators

## Common Uses

- One-off reports
  - Decision Support
  - Audit
  - Presentation (dressing up the output)
- Production Reporting
  - Download, format, report, believe
- What do your enterprises use it for?

## When End User Computing Goes Wrong....

- What are the impacts?
  - The Croll Scale...

### Impact of Error, loss, improper disclosure

- **Critical** ... could compromise a government, a regulator, a financial market, or other significant public entity and cause a breach of the law and/or individual or collective fiduciary duty. May place those responsible at significant risk of criminal and/or civil legal proceedings and/or disciplinary action.
- **Key** ... could cause significant business impact in terms of incorrectly stated assets, liabilities, costs, revenues, profits or taxation etc. May place those responsible at risk of adverse publicity and at risk of civil proceedings for negligence or breach of duty and/or internal disciplinary action,
- **Important** ... could cause significant impact on the individual in terms of job performance and career progression without directly, greatly, immediately or irreversibly affecting business or the organization.
- **Store & Retrieve** ...used as databases, with few issues other than data correctness and information security & where the impact is low.
- **Expired** ...over three years old no longer required in the active management of the business, but may be required to be archived by statute or good practice. Present impact is low.
- **Personal** ... used by the individual in the day-to-day performance of their duties, where the impact is low.

- **Critical** ... could compromise a **government, a regulator, a financial market, or other significant public entity** and cause a breach of the law and/or individual or collective fiduciary duty. May place those responsible at significant risk of criminal and/or civil legal proceedings and/or disciplinary action.

- **Key** ... could cause **significant business impact** in terms of incorrectly stated assets, liabilities, costs, revenues, profits or taxation etc. May place those responsible at risk of adverse publicity and at risk of civil proceedings for negligence or breach of duty and/or internal disciplinary action,

- **Important** ... could cause **significant impact on the individual** in terms of job performance and career progression without directly, greatly, immediately or irreversibly affecting business or the organization.
- **Store & Retrieve** ...used as databases, with **few issues other than data correctness** and information security & where the impact is low.

- **Expired** ...over three years old **no longer required in the active management of the business**, but may be required to be archived by statute or good practice. Present impact is low.
- **Personal** ... **used by the individual** in the day-to-day performance of their duties, where the impact is low.

## When End User Computing Goes Wrong....

- What are the impacts?
  - The Croll Scale...
  - Types of serious Impact
  - Error
  - Security
- What's YOUR experience?

## More on impacts -

- Domain Specific
- Errors in PERSONAL applications can kill people
  - Doctors – miscalculating drug dosage
  - Used by engineers can lead to structural failure through design errors
- Errors in PERSONAL Applications can kill companies & Careers
- Discuss?

## Control Approach

- Understand what's out there
  - Catalogue the applications
  - This can be automated
- Risk Assess it
  - Use Impact first
  - Then estimate likelihood
  - Policies, training, testing, developer knowledge
  - Use relevant CobIT maturity models
- Recommend Treatment (s)

## Likely Incidence of Errors

- Organisation Questions
- Domain Questions
- Specification & Design Questions
- Testing Questions
- Documentation Questions
- Questions re. complexity of the application
- Data Control & security Questions

# Maturity Models for Self-Assessment



## *Maturity Levels*

### 0 Non-existent

There is no process for designing and specifying end-user developments. Typically, end-user computing is performed in an unstructured manner by untrained end-users, with little or no documentation of actual requirements and no testing.

***There is an extremely high risk of error in important EUC Applications.***

## *Maturity Levels*

### 1 Initial / Ad Hoc

There is an awareness that a process for developing end-user applications is required. Approaches, however, vary from development to development without any consistency and typically in isolation from each other. The organisation's business depends upon a variety of individual solutions with varying degrees of documentation and control and now suffers legacy problems and inefficiencies with maintenance and support.

***There is a very high risk of errors in important end-user applications.***

## *Maturity Levels*

### 2 Repeatable but Intuitive

There are similar processes for developing and maintaining end-user applications, but they are based on the expertise within the users, not on a documented process. The success rate with end-user applications depends greatly on individual users' skills and experience levels. Maintenance is usually problematic and suffers when internal knowledge has been lost from the organisation.

***There is a high risk of errors in important end-user applications***

## *Maturity Levels*

### 3 Defined Process

There are documented development and maintenance processes. An attempt is made to apply the documented processes consistently across different end-user applications, but they are not always found to be practical to implement. They are generally inflexible and hard to apply in all cases, so steps are frequently bypassed. As a consequence, end-user applications are often developed and implemented in a piecemeal fashion. Maintenance follows a defined approach, but is often time-consuming and inefficient.

***There is medium risk of errors in important end-user applications.***

## *Maturity Levels*

### 4 Managed and Measurable

There is a formal, clear and well-understood end-user application development and implementation methodology and policy that includes a formal design and specification process, a process for testing and requirements for documentation, ensuring that all end-user applications are developed and maintained in a consistent manner. Formal approval mechanisms exist to ensure that all steps are followed and exceptions are authorised. The methods have evolved so that they are well suited to the organisation and are likely to be positively used by all staff, and applicable to most important developments.

***There is a low risk of errors in important end-user applications.***

## 5 Optimised

End-user applications are developed and maintained in line with the agreed processes. The development and maintenance process is well advanced, enables rapid deployment and allows for high responsiveness, as well as flexibility, in responding to changing business requirements. The end-user application development and implementation process has been subjected to continuous improvement and is supported by internal and external knowledge databases containing reference materials and best practices. The methodology creates computer based documentation in a pre-defined structure that makes production and maintenance very efficient.

*There is a very low risk of errors in important end-user applications*

## Organisation Questions

- Is there an end-user application development policy ?
- Is it enforced ?
- Where's the ORGANISATION on the scale?
  - 0 – Non-Existent....
  - 5 – Flexible, used, enforced

## Domain Questions

- Does the developer understand the business issue being supported ?
- For the DEVELOPMENT...
  - 0 – Blind Guesswork....
  - 5 – Recognised as an expert

## Specification Questions

- Is there a written specification ?
- Is it adequate ?
- If not, how does the developer know the application is right ?
- For the DEVELOPMENT ...
  - 0 – Non-Existent....
  - 5 – Current, Comprehensive

## Design questions

- Is there evidence of design?
- Consistent style?
- Meaningful colour, format, annotation?
- For the DEVELOPMENT ...
  - 0 – Non-Existent....
  - 5 – Clear and consistent

## Design

- Rate the DEVELOPMENT as a whole on the following criteria. Use a scale of 1 to 5, where 1 means “least positive” and 5 means “most positive.”.
  - Overall ease of understanding
  - Use of modules
  - Use of parameterisation
  - Ease of use
  - Ease of communication

## Testing Questions

- Was the development tested ?
- Adequately ?
- Have changes been tested ?
- Where are the results ?
- For the DEVELOPMENT ...
  - 0 – No formal testing....
  - 5 – Original and all changes thoroughly tested; tests evidenced

## Testing

- Test cases ?
- Test data sets with known correct answers
- Proof of testing
- Extreme inputs
- Data Sensitivity
- Usability
- Calculation Accuracy

## Calculation Accuracy

- Test against
  - Known Results
  - Simple Inputs
  - Invalid data
  - Extreme Data
  - Empty Cells / Zero Values
- Automated test harnesses are available

## Documentation Questions

- Is the development documented ?
- Is the documentation
  - Comprehensive?
  - up-to-date?
  - Adequate?
- Has it been updated after changes?
- For the DEVELOPMENT ...
  - 0 – Non-Existent....
  - 5 – Current, Comprehensive

## Documentation Contents

- Look for...
  - assumptions
  - Sources for inputs
  - Guide to modules / screens
  - Comments in code

## Complexity Questions

- Is the application a complex solution to a simple problem ?
- Is it necessarily complex ?
- The likelihood of error rises with complexity
- For the DEVELOPMENT ...
  - 0 – Unnecessarily complex
  - 5 – Simple and robust

## Data Control Questions

- What controls ensure that data handled in the application is
  - complete?
  - relevant?
  - accurate?
  - timely?
- For the DEVELOPMENT ...
  - 0 Non-Existent....
  - 5 Comprehensive, documented controls in place

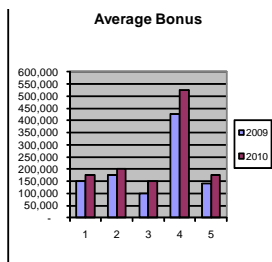
## Data Controls to Look For...

- Cross-check of totals
- Control Totals
- Validation Formulas
- Reasonableness tests for automated uploads
- Error Trapping for incorrect data types
- Protected cells / worksheets in spreadsheet applications
- Hiding unused features

# Security Issues

- Can EUC let data leak?
- Can EUC corrupt the database?
  - Careless SQL costs integrity!

# Security



ABC Co Director's Pay		
	2009	2010
Smith	150,000	175,000
Jones	175,000	200,000
Bloggs	100,000	150,000
Total	425,000	525,000
Average	141,667	175,000

The graph is embedded in the slide as an editable object – so the Table can be made visible causing inadvertent (we hope) leakage of Sensitive personal/ commercial information...

## Security

- What are you distributing with your documents? Have you purged all marked-up revisions in the text? What's in the document properties?

Here is some entirely harmless information in a Word document

~~Here is something really embarrassing that was removed at the drafting stage~~

## Risk Treatments / Controls

- Our end users have no clue. And that's our fault.
- If we don't teach the people we're responsible for to take care of themselves - - just a little bit -- we are going to continue spending the majority of our time cleaning up perfectly preventable computing tragedies. This is important.
  - Linda LeBlanc (eSecurityplanet.com via K-NET)

## Education, Education, Education

- About the tools
  - Do users know how to use them?
  - Trained – More than button pressing – design
- About the data
  - Do users understand the data using?
  - What do the elements MEAN?
  - Effective Dates?
  - Current\_Value – How defined?

## Treatment Approach

- Understand the risks
- Make Sure Users understand the risks
- Prioritise
- Understand the tool
- Understand the Data being manipulated
- Application level controls
  - Completeness,
  - Accuracy,
  - Authorisation

## Use Protective Markings

- HM Government Protective Marking System
- 5 Markings...
  - TOP SECRET
  - SECRET
  - CONFIDENTIAL
  - RESTRICTED
  - PROTECT
- NOT PROTECTIVELY MARKED used to indicate positively that a protective marking is not needed
- (and has not been forgotten)
  - Cabinet Office; Security policy Framework

## Risk Treatment

- For Critical, Key, and Important applications
  - Impose Policy & Standards
    - Specification
    - Testing
    - Layout – Common look and feel in the organisation
    - Security

## Risk Treatments

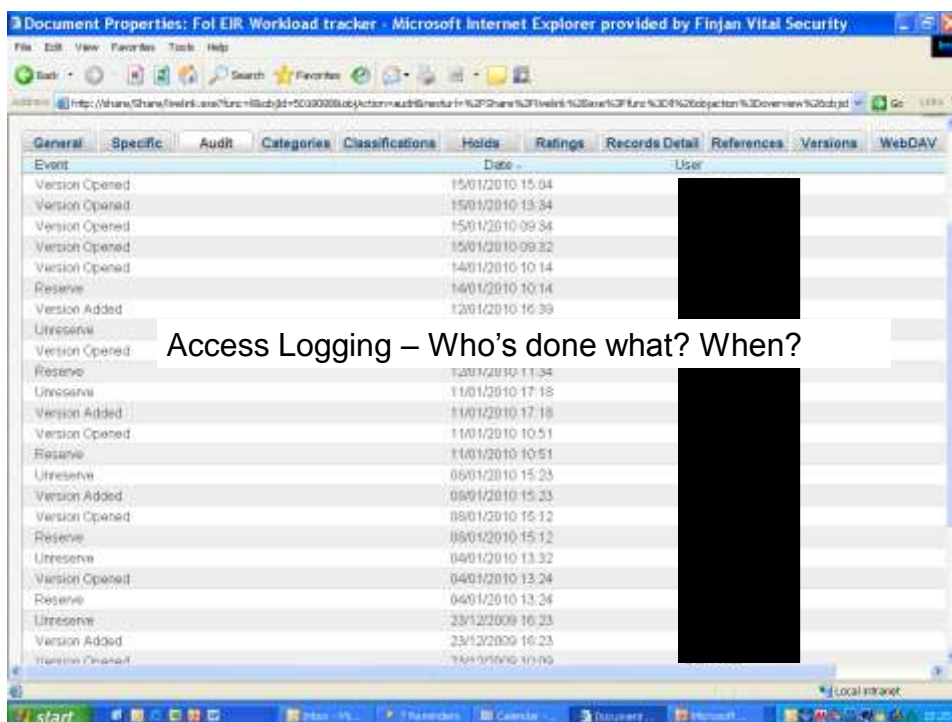
- Security
  - Access TO Applications & Data
    - File system security
    - File open password
  - Secure “Master” copy
  - Ability to change
    - Use spreadsheet / document protection
    - Password protect source
    - BUT – Easily circumvented

## Availability

- How can we ensure end-user information is...
  - Retained?
  - Available?
  - Traceable?
  - Definitive?
- How can we tell who’s done what with our information?

## Electronic Document & Record Management Systems

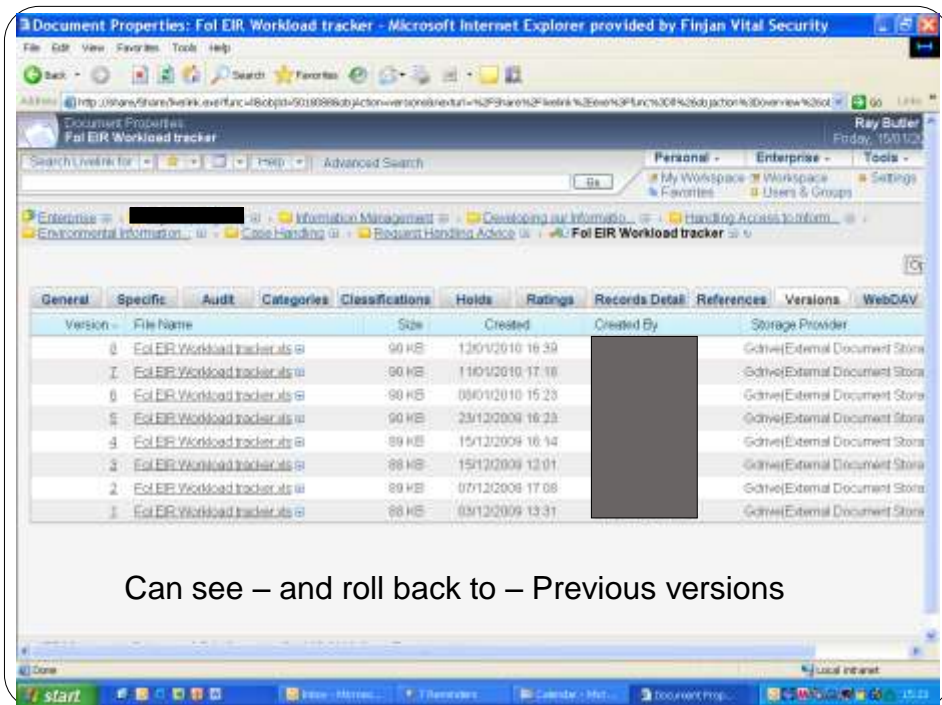
- Manage storage & retention
- Sophisticated access controls
  - Unauthorised users may not even see sensitive material
  - Rights Management
  - Locks records (as opposed to documents)
  - Logs changes (Versioning)
  - Logs Access



The screenshot shows a document properties window titled "Document Properties: FoI EIR Workload tracker - Microsoft Internet Explorer provided by Finjan Vital Security". The window displays an audit log with the following columns: Event, Date, and User. The log contains 20 entries of document activity, including versioning and retention events. The User column is redacted with black boxes.

Event	Date	User
Version Opened	15/01/2010 15:04	
Version Opened	15/01/2010 13:34	
Version Opened	15/01/2010 09:34	
Version Opened	15/01/2010 09:32	
Version Opened	14/01/2010 10:14	
Reserve	14/01/2010 10:14	
Version Added	12/01/2010 16:39	
Unreserve		
Version Opened		
Reserve	12/01/2010 11:34	
Unreserve	11/01/2010 17:18	
Version Added	11/01/2010 17:18	
Version Opened	11/01/2010 10:51	
Reserve	11/01/2010 10:51	
Unreserve	08/01/2010 15:23	
Version Added	08/01/2010 15:23	
Version Opened	08/01/2010 15:12	
Reserve	08/01/2010 15:12	
Unreserve	04/01/2010 13:32	
Version Opened	04/01/2010 13:24	
Reserve	04/01/2010 13:24	
Unreserve	23/12/2009 16:23	
Version Added	23/12/2009 16:23	
Version Opened	14/11/2009 10:00	

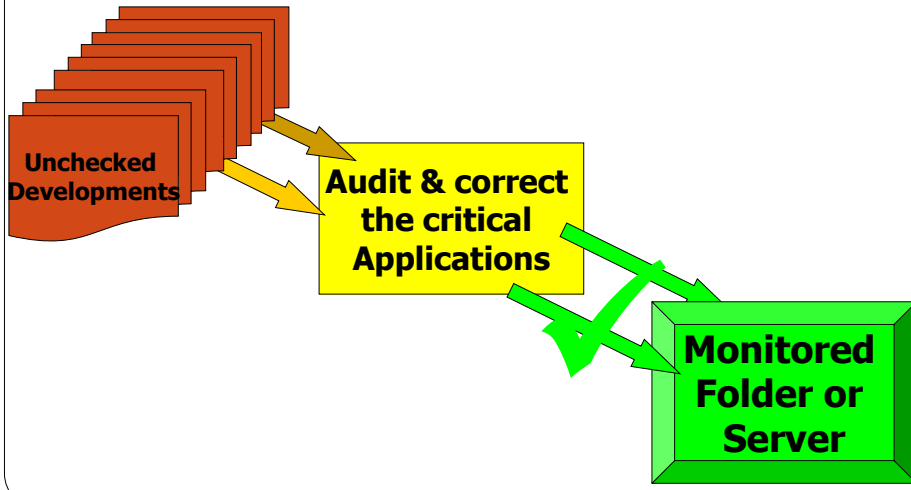
Access Logging – Who's done what? When?



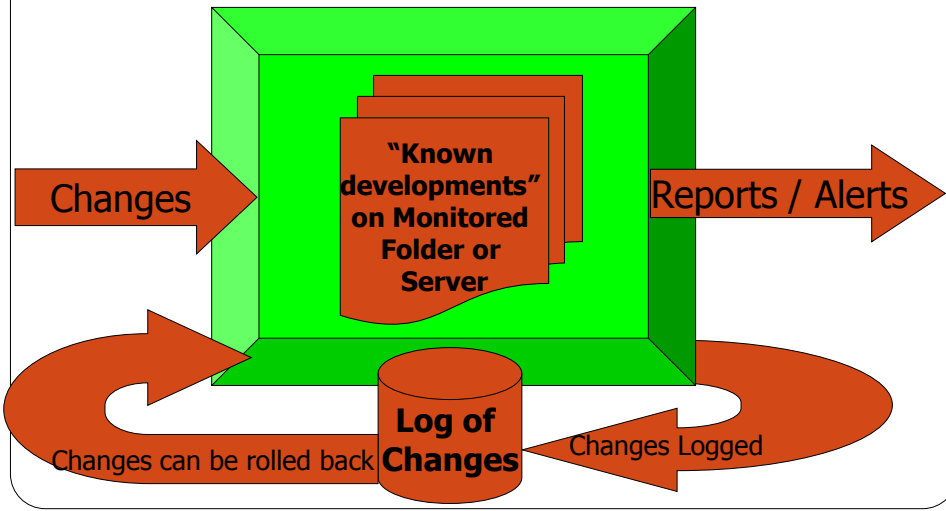
## Risk Treatments

- How can we keep End-user Applications correct?
- Continuous monitoring / auditing

## Continuous Audit for End-User Applications



## Continuous Audit for End-User Applications



## In Summary - Control Approach

- Understand what's out there
  - Catalogue the applications
  - This can be automated
- Risk Assess it
  - Use Impact first
  - Then estimate likelihood
  - Policies, training, testing, developer knowledge
  - Use relevant CobIT maturity models
- Recommend Treatment (s)

## Today's agenda

- Commonest end-user applications and the risks involved in their use
- Impacts of material error in the use of end-user applications
- A CobiT- based maturity model to measure the likelihood of material error from use of end-user applications
- Identify some good and not so good practices in end-user applications
- Describe some options for improving control of end-user applications.