End-User Computing Governance Policy

For User Developed Applications

November 2015

QUINTANT PARTNERS

Challenge Your Perspective

PUBLISHED BY

Quintant Partners
4 Chiswell Street
London
EC1Y 4UP

Any example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organisation, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This publication expresses the author’s views and opinions. The information contained in this document is provided without any express, statutory, or implied warranties. Neither the authors nor Quintant Partners will be held liable for any damages caused or alleged to be caused either directly or indirectly by this publication.

Authors: Guy Shepherd / Abbey Samyint

Template Version: 1.00

Contents

Introduction

End-user developed applications ("UDAs") now form an integral part of the information management and decision making framework of many organisations across different industry sectors. Unfortunately, gone unchecked, the end-user computing estate potentially presents a significant risk to ongoing business operations. The popular media is full of stories of financial loss & reputational embarrassment caused directly or indirectly with errors in end-user computing solutions.

What is End User Computing?

End-user computing ("EUC") refers to business applications which are designed, developed, maintained and used by the end-user business community outside the reach & control of the core IT function. These applications are usually developed using tools / software platforms which provide a flexible toolkit of powerful features but in a form which end-users can easily get to grips with. The most common of these tools is the spreadsheet, and the most of common software platform is clearly Microsoft Excel, but there are many others that can and do pose similar (or even greater) risks.

Why Do EUC Solutions Exist?

End-user developed applications exist for a variety of reasons, but without them, business operations would most likely grind to a halt. Some of the most common reasons for their development are listed below, in no particular order.

- Voids between industrial / enterprise systems – UDAs provide the "glue" to make end-to-end processes work
- Developed as prototypes for so-called industrial systems which never emerge, leaving the UDA as a production solution but without the corresponding level of control / governance
- End-user computing tools allow highly agile development and deployment of solutions without the hurdles (or discipline & governance) of formal project delivery lifecycles
- UDAs are considered cheap in relation to in-house developed or commercial off-the-shelf ("OTS") software, although the total cost of ownership and operation of end-user developed systems is difficult to quantify
- The end-user community is often not aware of alternative / better solutions and would rather develop something new than ask for support
- UDAs can be tailored to fit functional & non-functional requirements exactly – no compromises. Few if any commercial software packages offer such flexibility
- End-users potentially don't have access to a full selection of potential tools / necessary training
- IT may be unaware of business problems / need and / or unable to offer advice / support of right way to solve the problem
- Most end-computing tools offer a problematic convenience and ease of use / misuse

- UDAs are portable between users / teams and can easily be adapted / extended for different purposes
- UDAs allow users to feel they are adding value and contributing directly to business / functional success
- Many environments effectively encourage a make do and mend culture

Common Risks Associated with the EUC Estate

Unfortunately while user developed applications provide end-users with hugely powerful and flexible tools with which to carry out their business, they also present organisations with potentially significant operational and reputation risks that need to be understood and appropriately managed. Gone unchecked, the potential issues & errors associated with end-user computing can lead to reputational embarrassment, regulatory sanctions or even business failure. This has been noted by supervisory bodies across a range of industries (e.g. EIOPA), and recent / emerging regulations (such as Solvency II) are now actively encouraging (or forcing) organisations to understand and control the risks associated their end-user computing environments.

Some of the most common risks associated with end-user computing are shown below.

- Poor design / lack of testing
- Errors in of data, parameters, links & data sources
- Lack of audit trail of use / changes
- Fraud / access controls / confidentiality
- Missing / inappropriate security
- Capacity / performance / scalability problems
- Availability / DR – local / individual data share rather than corporate network
- Appropriateness of tooling / technology for requirements
- Understanding / documentation / peer awareness
- Skill of developers / users
- Complex / invisible dependencies
- Complexity / over-engineering of solution
- Ownership - especially when things go wrong – not IT's problem!
- Silos of knowledge
- Evidence of change, testing and development standards
- Currency of calculations / data / logic (particularly important for length calculation cascades)

Emerging Issues for Financial Services

With the increased focus on risk management and control, financial services organisations are now having to respond to demands for evidence of controls around user developed applications in the same way as auditors & regulators expect to see robust governance around enterprise systems. Some of these demands might include the following:

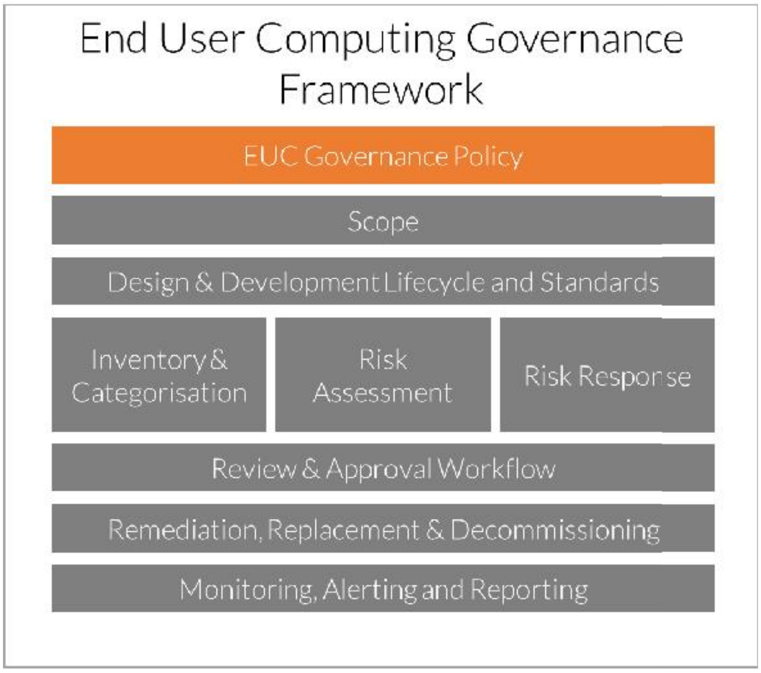
- Can you list the spreadsheets (or other UDAs) that are used (and how they are used) as part of the regulatory reporting cycle?
- What level of control / governance is appropriate to apply to each of these spreadsheets?

- Demonstrate that the UDAs have been designed, developed, tested and changed in a robust manner during the period
- Who has access to change a specific UDA?
- How have the results from a calculation cascade changed during the period? Was this change appropriate / anticipated?
- Is an audit trail of changes / impact of changes available for all critical reporting UDAs?

Obviously addressing such challenges might present a significant burden to business functions which are already busy using the UDAs to complete business critical activities.

What's the Answer?

In order to understand and mitigate the risks associated with the end-user computing environment and respond to the emerging audit / regulatory demands, we recommend adopting the approach outlined below.



End User Computing Governance Framework

EUC Governance Policy

Scope

Design & Development Lifecycle and Standards

Inventory & Categorisation

Risk Assessment

Risk Response

Review & Approval Workflow

Remediation, Replacement & Decommissioning

Monitoring, Alerting and Reporting

Fundamental to this approach is the adoption of an overarching end-user computing governance policy to be applied & enforced organisation-wide or at least across those functions of an organisation relying on UDAs for critical / regulated business processes.

Use of Governance Technology

Depending on the extent to which end-user computing plays a role in supporting critical business processes, it may be appropriate to consider the use of specific technology offerings to help implement and monitor the governance framework. While tools, such as Enterprise Spreadsheet Management solutions can undoubtedly help ensure governance is appropriately implemented and maintained, it's important to understand that such tools only provide part of the solution, and must be supplemented by other (non-technology) solutions. Similarly, all governance technologies require ongoing support & maintenance which needs to be carefully considered before adoption.

Structure and Use of This Policy

This policy template is design to be adapted to meet the needs of a specific organisation and dovetail with any existing risk management policies and procedures. Similar the policy is designed to be used either in isolation or in conjunction with a variety of technology solutions designed to help control the end-user computing environment on an ongoing basis.