Deloitte.

End User Computing
Solving the problem

Introduction

End User Computing (EUC) applications (such as Microsoft Excel, Microsoft Access, and others) continue to present challenges for organizations.

On the one hand, EUCs provide a great benefit by allowing users to directly manage, control, and manipulate data. Unlike SAP, Oracle, and other Enterprise Resource Planning (ERP) applications that facilitate the automated and integrated flow of transactions and data, EUCs are neither ponderous nor difficult to modify. In fact, EUCs allow businesses and users to quickly deploy solutions in response to shifting market and economic conditions, industry changes, or evolving regulations. They can also help plug functionality gaps for ERP systems.

Alas, those same elements that make EUCs so appealing (and vital in providing timely information) can also make them challenging to manage and control effectively. User-developed and user-controlled applications, by definition, are not subject to the same development, monitoring, and reporting rigor and control as traditional applications. And often, management lacks visibility into exactly how pervasive the use of EUCs has become throughout the enterprise.

What types of issues are companies facing?

Challenges associated with EUCs include:

- Misstated financial statements due to simple data entry or calculation errors in spreadsheets
- Regulatory and compliance violations (see exhibit A for a list of regulations that could potentially impact EUCs)
- Operational impacts and losses due to errors
- Loss of time stemming from cumbersome manual processes and calculations that could be automated
- Data redundancy and version control
- Lack of recovery or forensic capabilities
- Higher risk of fraud
- Audit findings due to lack of control around EUCs

These issues are not new; organizations are typically very aware of the issues they have experienced with EUCs internally, and a quick Internet search will highlight a number of high-visibility breakdowns in EUC controls resulting in restatements and/or fraud.

What has changed?

The promulgation of Sarbanes-Oxley and other internal control regulations around the globe heightened the awareness that EUC controls were needed. Some organizations responded proactively, putting measures in place to address the issues. Others did little, unless the issues were directly forced upon them by regulators, auditors, or reporting errors that came to their attention. However, in both cases, many of these measures proved to be insufficient in resolving the set of challenges posed by EUCs. And reporting errors, audit findings, and other issues continued to arise. Moreover, recent changes in the business environment continue to increase the need for EUC controls, including:

- The economic downturn curbed investment in information technology (IT), resulting in a dramatic increase in the development and use of EUCs to address business needs not being addressed by IT.
- Macroeconomic financial crises have increased the level of scrutiny by auditors and regulators around EUCs, particularly those that perform financial modeling.
- Workforce reduction has impacted the number of employees with knowledge of how the EUC functions, which makes troubleshooting, error identification, and changes difficult.
- EUC technologies continue to increase in ease of use and functionality, making it easier for users to quickly deploy robust and complex EUC solutions.

The current state

Most organizations are aware of the challenges presented by EUCs and the need to address them. As mentioned earlier, many companies have taken measures to deal with these issues. Unfortunately, these measures have often been ineffective, for a variety of reasons. Many organizations have chosen to develop and disseminate internal policies regarding the use of EUCs. But as with most policy-based solutions, there are significant challenges when it comes to enforcing and monitoring compliance.

Other organizations have attempted to address the problem through the heavy use of technology, by purchasing and implementing tools or other technical solutions that can provide controls and enforce compliance. Although these tools are helpful, and often necessary, without the corresponding organizational structure and personnel to support the functionality of the tool, these solutions tend to be under utilized and ineffective.

Another approach is to allow each business unit to address the issue independently. This often leads to inconsistent levels of control, as well as duplication of effort and inefficiencies.

The purpose of this whitepaper is not to throw stones at the progress that has been made. In fact, this is a fairly typical maturation of organizational capability that we have seen in various other disciplines throughout the enterprise. Business issues emerge, technology enablers become more robust, and the enterprise moves over time from a chaotic, uncontrolled approach; to a repeatable approach; and, finally, to an optimized and automated approach. Our purpose is to lay out an objective model that will provide organizations with a framework for addressing issues while managing and controlling EUCs holistically, leading to an advanced state of highly effective EUCs that support business processes in an error-free manner.

The solution

Our experience leads us to conclude that point-specific solutions are not effective. Trying to solve the EUC controls challenge by merely establishing and announcing a policy, or by throwing technology at the problem, does not provide an effective and sustainable solution. Additionally, every organization uses EUCs differently and for a variety of purposes. Consequently, there is no single cookie-cutter approach that will work for all.

That being said, a sustainable and effective approach to controlling EUCs is achievable. In order to accomplish this objective, companies should deploy a holistic enterprise-level program for managing EUCs. While the specifics of such a program will vary from organization to organization, the fundamental elements of the program are consistent across enterprises. It is our experience that companies that develop and deploy a holistic EUC management program are much more likely to accomplish their EUC management objectives in a timely, effective, and efficient manner. Those that continue to pursue point-specific solutions will remain mired in inefficiency, and they will continue to be frustrated by errors and recurring issues.

Effective EUC management programs comprise elements of governance, process, people, and technology. Each of these elements should be customized to meet the specific needs of the organization. A brief overview of the programmatic framework and key considerations is listed on the next page.

	Key elements	Description	Items to consider
Governance	Definition and identification of EUCs	The statement that defines what constitutes an EUC. The definition generally distinguishes EUCs from IT-developed and supported applications and will determine which EUCs should be placed under management. This is critical to define the scope of the EUC compliance program. 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?	• What decision criteria are used to determine whether an application should be considered an EUC? • How does your organization define EUCs? • Is there another method by which EUCs are classified?
	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.	• Is there a formal policy in place that establishes a consistent framework for the control of EUCs within your organization? • Is the policy applicable to the whole organization, or is it focused on particular business units?
	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.	• Is a governance model in place that specifically defines the ownership of EUCs? • Is this is a centralized, decentralized, or hybrid model?
	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.	• Has your organization identified key metrics to be tracked and distributed to its stakeholders and senior management? • Have reporting tools been configured to support the reporting metrics and objectives?
People	Roles and responsibilities	Identify the key stakeholders in the EUC management program. 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.	• Have the EUC stakeholders been identified? • Are roles and responsibilities of the various stakeholders of EUCs clearly defined? • Are the responsibilities of a program sponsor, central program group, steering committee, business unit representation, etc. defined?
	Training and awareness	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.	• Does your organization have a formal awareness and/or training program that addresses EUC-related activities? • Who is responsible for managing and deploying these training programs?

	Key elements	Description	Items to consider
Process	Risk ranking and prioritization	**Define risk ranking framework** 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.	• Has a risk ranking framework been defined? • If defined, has the risk ranking criteria been applied to existing EUCs?
		Application of risk ranking framework 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	• How was the application of risk criteria performed; what steps were taken to prevent "gaming the system" to avoid additional controls requirements?
	Inventory	**Define an inventory approach** The process of inventorying EUCs often proves to be one of the most challenging and time-consuming elements of the EUC management program. 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.	• Have you defined an approach on how to organize the EUC inventory process — by business unit, geography, etc? • Is there a central repository in place at this time? • Does the central repository contain inventory across all business units of the company? • Have technical support requirements been defined (e.g., use of tools, native search features in the network, or via a manual process)? • Who is responsible for managing the central repository?
		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.	

	Key elements	Description	Items to consider
Process	EUC controls	Based on the selected EUC risk model, the organization should define an EUC controls standard that will be implemented for identified EUCs. This standard should be aligned with the risk ranking process. For example, the required control standard for an EUC determined to be high-risk may be different than an EUC determined to be medium-risk. Examples of required controls should include the following: • **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.	• Has your organization defined an EUC control standard? • Does the EUC control standard align with the risk ranking process, as well as other required controls (e.g., Sarbanes-Oxley)?
	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.	• Has your organization created templates as part of the EUC program? • Are templates required for all newly created EUCs? • Are legacy EUCs required to be converted into the templates?
	Baselining	Baselining is an important step in EUC management. 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.	• Does your organization have a defined process for baselining and approving baselined EUCs? • Does your baselining process cover only newly created EUCs going forward or are legacy EUCs baselined as well? • Who is responsible for performing the baselining exercise? Are sufficient resources deployed in this regard?

	Key elements	Description	Items to consider
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.	• Who performs the testing to monitor the effectiveness of EUC controls? • How often is the testing performed? • To whom are the reports of effectiveness addressed? • Who is responsible for addressing remediation?
Technology	**Technology support strategy**	Any organization attempting to put a high number of EUCs under management (e.g., >200) will experience difficulties without the support of technology enablers. A strategy should be defined for the use of technology enablers supporting inventorying processes, analytical review during baselining and enforcing controls. Specific EUC management software tools can be deployed, or native functionality (such as Microsoft SharePoint) can be used, with various degrees of functionality available. The strategy should balance cost with benefits.	• How will the EUCs and related controls be managed? Manually, using native functionality, or via automated tools? • Has an overall technical strategy for EUC management been defined?

	Key elements	Description	Items to consider
Technology	Define technology requirements	**Technology 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?)	• Have technical requirements been defined? • Were existing native technical capabilities evaluated? • Were vendor tools considered?
		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. For example, will one enterprise server be used, or will each global region have a separate server for managing EUCs?	• How were sizing requirements defined? • Did sizing requirements consider EUC iterations (e.g., daily versions of the same EUC)? • Was IT involved in sizing discussions? • Will EUC infrastructure components be centralized or distributed (by geography or business unit)?
		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.	• Has a security strategy and role design framework been established? • Have security roles been evaluated for segregation of duties conflicts? • Have supporting security and user-administration processes been defined? • Do security requirements align with overall enterprise security policies and standards?
		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.	• Has an enterprise rollout strategy been defined and agreed to by stakeholders? • Will compliance requirements be rolled out by geography or business unit? Or another method? • Have EUC inventory results been evaluated in conjunction with rollout strategies and project timelines? • Have staffing requirements for rollouts been evaluated?

The framework above does not provide all the potential requirements that a company might need when establishing an enterprise-level programmatic approach to managing EUCs. But in our experience, programs that lack any single criteria listed above are far less effective.

As you have seen simplified above, many of these criteria have a high degree of flexibility and optional methods for deployment. Consequently, you should not minimize the amount of planning and strategizing that will be needed to define the specifics of the program within your enterprise. Also, the amount of time needed to bring EUCs under management of the program will be extensive. Most organizations find that this can be a multi-year project, which requires constant fine tuning and updating as the organization continues to evolve.

Benefits of an enterprise EUC program

The main objective of an enterprise EUC program is risk management. As with most risk management initiatives, the benefits (particularly those with hard dollar savings) can be difficult to quantify. However, many organizations that have deployed such programs have experienced bottom-line benefits in addition to risk mitigation, and they have developed business cases that demonstrate real ROI. Our experience with such programs leads us to conclude that the following benefits can result:

- Reduced errors in preparation of financial statements and management reporting, resulting in faster closing processes and reduced staff time to research and remediate issues.
- Reduction in direct identified losses due to errors.
- Reduction in testing requirements and fees by auditors. Rather than needing to test each EUC or a large sample of critical EUCs, auditors can test management and program controls over EUCs, particularly when an automated tool has been deployed.
- Reduced regulatory and compliance penalties.
- Reduced training and on-boarding requirements for new employees.
- Elimination of redevelopment work needed to re-create EUCs when key employees leave or when the EUC is lost.
- Opportunities to eliminate certain EUCs completely by identifying those that are organizationally entrenched but serve no direct business need, or that can be replaced by existing ERP functionality.
- Reduced effort to remediate errors in EUCs.

Conclusion

End User Computing continues to present both challenges and opportunities for organizations. Companies will continue their efforts to migrate functionality from EUCs into ERP packages or other more controlled business applications, but EUCs will not be going away anytime soon. Companies are too dependent on EUC functionality that allows them to respond quickly and effectively to dynamic market conditions. And auditors and regulators will continue to make EUCs a priority when evaluating and assessing organizations.

Consequently, companies should deploy tools and techniques to effectively manage and control the EUCs that are critical to financial reporting or operations. Progress made by organizations to date suggests that policy-based or point-specific solutions are ineffective in helping to mitigate the array of risks posed by EUCs. A better alternative is to design and deploy a holistic enterprise-level program that effectively comprises elements of governance, people, process, and technology. Companies that do so will find that such a program contributes to overall risk management and bottom-line benefits.

Appendix

Exhibit A

A sampling of laws and regulations potentially affecting EUC management		
Law or regulation	**Issuing authority**	**Primarily applies to**
21 CFR Part 11- FDA	US	FDA-regulated industries – Drug makers, medical device manufacturers, etc.
AS5	US	Public companies
Basel II/III	EU/International	Banks and financial institutions
California SB 1386	State of California	All companies doing business in the State of California
Centers for Medicare & Medicaid Services (OIG)	US	Firms benefiting from Retiree Drug Subsidy (RDS) program
CSOX (Canada)	CA	Public companies in Canada
Data Protection Act of 1998	UK	Companies doing business in the UK
DoD 5015.2	US	Government contractors
Dodd-Frank Act	US	Public companies
European privacy regulations	EU	Companies doing business in the European Union
FASB	US	Public companies

A sampling of laws and regulations potentially affecting EUC management		
Law or regulation	**Issuing authority**	**Primarily applies to**
Financial Industry Regulatory Authority (FINRA)	US	Securities firms
Germany's law on employee confidentiality	DE	Companies doing business in Germany
Gramm-Leach-Bliley Act (GLBA)	US	Financial institutions
HIPAA	US	Companies that handle healthcare information
Japan's Financial Instruments and Exchange Law	JPN	Banks and financial institutions
Markets in Financial Instruments Directive (MiFID)	UK	Banks and financial institutions
NAIC Model Audit Rule	US	Insurance companies
OMB Circular A-123	US	Federal agencies
Patriot Act	US	Companies doing business in the U.S.
PCI DSS	US	All companies that handle credit card information
Solvency II	EU	Insurance companies operating in the EU
Sarbanes-Oxley	US	Public companies

Contacts

Michael Juergens
Principal
Deloitte & Touche LLP
+1 213 688 5338
michaelj@deloitte.com

Tom Donohue
Senior Manager
Deloitte & Touche LLP
+1 702 301 9976
tdonohue@deloitte.com

Clayton Smith
Senior Manager
Deloitte & Touche LLP
+1 303 298 6739
claysmith@deloitte.com