SOCIETY OF ACTUARIES

Article from:

CompAct

April 2013 – Issue No. 47

Overview of Programmatic Framework and Key Considerations

	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.	
	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)?

	Key elements	Description	Items to consider
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.	• 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?
	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?