Deloitte.

End User Computing: Risks of Convenience

Clayton Smith, Senior Manager
Deloitte & Touche LLP
January 24, 2013

Table of Contents

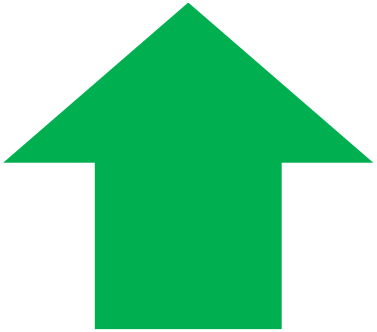
End User Computing (EUC) Introduction

EUC Control Environment

Questions & Answers

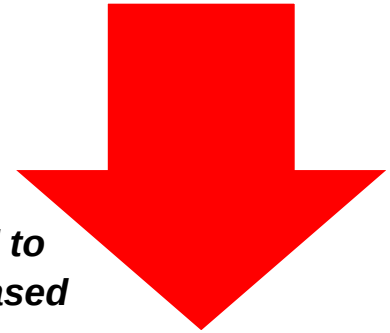
EUC Introduction – The Risks with EUC Usage

The appeal and convenience of EUC usage can often result in non-controlled processes that increase organizational risk.



ERP Environment

- Established Controls
- Well Defined Procedures and Ownership
- Auditable



EUC Environment

- Uncontrolled Change
- Limited Security Options
- Incomplete Version Control

NOTE: This decrease in control can lead to organizational losses including an increased risk of the following:

- ***Misstated Financial Statements***
- ***Regulatory and Compliance Violations***
- ***Negative Operational Impacts***
- ***Increased Fraud Risk***

EUC Introduction – Current State

Most organizations are aware of the risks associated with the use of EUCs (often documented during audits as the "Key Spreadsheets") usage and have made attempts to implement policies and procedures to control the usage of these EUCs.

Organizational Challenges

Governance

- What is an EUC (Spreadsheet, Data Repository, Database), organization cannot agree
- Who owns the organizational control / use of EUCs
- The organization cannot agree on a standard use of these EUC technologies

Technology

- Network security is limited and cannot provide granular control of EUCs
- Audit logging is currently not available on standard EUC solutions (Excel, Access, etc…)
- Inconsistent technologies are used throughout the organization.

Process

- Departments have established and implemented inconsistent processes for EUC usage
- The organization does not have a clear way of determining which EUCs should be controlled (each department has their own way of doing things)

People

- There is no clear ownership of the EUCs
- Due to organizational turnover, initial EUC design and intent have been lost
- A lack of EUC usage guidelines and training result in inappropriate usage / changes of EUCs

Table of Contents

EUC Introduction

EUC Control Environment

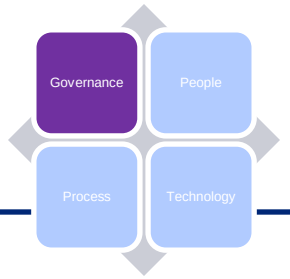
Questions & Answers

EUC Control Environment – Determine a Framework

Every organization is unique and a "one-size fits all" approach to EUC control is inappropriate. To help ensure that the EUC control environment is designed appropriately, management should first determine a framework.

The Four Cornerstones of an EUC Control Framework

EUC Control Environment - Governance



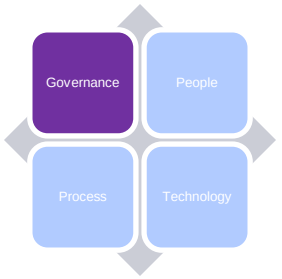
Defining EUCs

- In order to establish appropriate scoping, management should first define what constitutes an EUC
- Determine a list of applications that are currently in use by the user group. Often times, management does not consider the full population of potential EUCs, restricting their scope to spreadsheets alone. Often times users make use of other types of EUCs, including user controlled databases (such as Access), non-approved programming languages (VB Scripts, APIs, etc.)
- Once a full population of EUCs has been determined, management should determine which of these EUCs is impacting the organization (operationally or financially).
- Management should assess the usage of these EUCs and determine if standard procedures are followed (it is likely, due to the disparate usage, that usage of these EUCs is not consistent).

Policies and Standards

- In order to drive consistent usage of EUCs, management should develop comprehensive policies and procedures.
- Management should evaluate existing policies and procedures (often developed within business groups) and work to establish and propagate an organization wide version.

EUC Control Environment - Governance



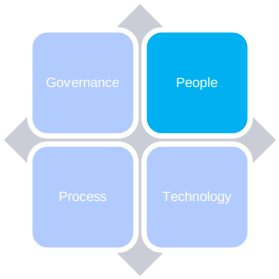
Ownership

- Determine how EUC management will be structured within the organization.
  - Centralized – All EUCs are managed by a centralized team. Changes, access, standardization and reporting is owned by a single team.
  - De-Centralized – EUCs are managed by individual business units. Changes, access, standardization and reporting is owned by multiple leaders throughout the organization.
  - Hybrid – EUC ownership is split. Standardization, reporting and compliance is managed by a centralized team. Changes and access are managed by multiple leaders throughout the organization.
- Management should evaluate the current ownership model and determine if it will meet the long term framework goals.

Monitoring and Reporting

- Management should define key risks and metrics for EUCs.
- Management should establish an appropriate reporting mechanism, conducive to supplying meaningful information to spreadsheet stakeholders.

EUC Control Environment - People



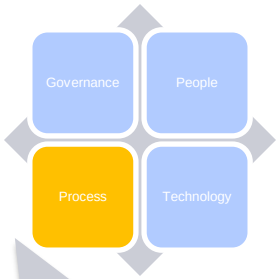
Roles and Responsibilities

- Leadership and organizational buy-in are key to establishing a successful EUC framework. To increase the likelihood of success, management should identify key stakeholders
- Once key stakeholders have been defined, they should be assigned roles and responsibilities
  - Program Sponsor
  - Central Program Group
  - Steering Committee
  - Business Unit Representative
  - EUC Users Administrators

Training and Awareness

- Establish a formal training program for each of the Key Stakeholder Roles
- Target the training timeline to be consistent with the framework goals

EUC Control Environment - Process



A phased approach enables organizational buy-in and streamlines the implementation of the process

Phase I – Define EUC Risk Ranking Metrics

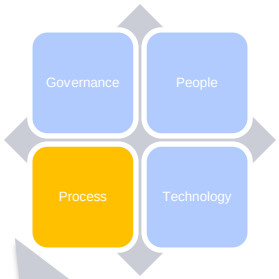
Phase II - Evaluate EUC Population and Determine Scope

Phase III - Design EUC Specific Controls

Phase IV - Apply Controls to the In-Scope EUCs

Phase V - On-Going Control

EUC Control Environment - Process



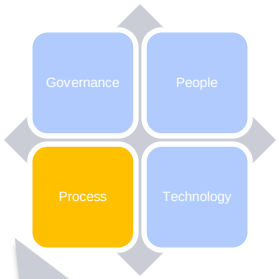
Very likely, a majority of the EUCs that exist within the organization do not have a significant impact (operationally or financially). Management should consider defining risk criteria to determine if an EUC should be included in the program.

Phase I –
Define EUC Risk Ranking Metrics

Common metrics used to determine the overall risk of an EUC are:

- Output Materiality
- Throughput Amount
- Overall Complexity
- Judgment Applied in Usage

EUC Control Environment - Process

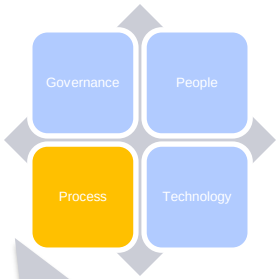


When organizations perform an initial inventory, they are often overwhelmed at the number of EUCs that exist (known to be upwards of 10,000.) Typically, management can exclude a majority of these EUCs with basic judgment.

Phase II - Evaluate EUC Population and Determine Scope

Once an appropriate population of EUCs is defined, management should apply risk thresholds (using the matrix defined in Phase I) to isolate the high risk EUCs to enroll in the program.

EUC Control Environment - Process



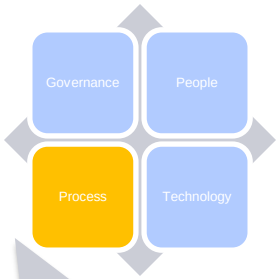
In order to reduce the risk of EUC errors that result in misstated financial statements, regulatory and compliance violations, negative operational impacts and increased fraud; management should design EUC specific controls.

Phase III -
Design EUC
Specific Controls

Common EUC controls may include the following areas:

- Data Integrity Control
- Change Control
- User Access and Restriction Control
- Version Control
- Availability Control

EUC Control Environment - Process

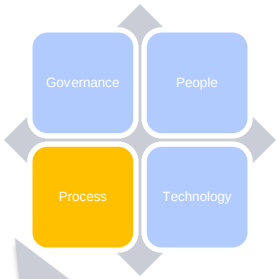


Once management has agreed to an appropriate control environment, a roll-out methodology should be designed. Often times, this is best achieved by the use of templates (standard structures designed to enable smooth transition into the control environment).

Phase IV - Apply Controls to the In-Scope EUCs

The application of controls typically has a significant impact on the user group. Often times, this phase of the process is underestimated. It can be difficult to estimate the time to implement these controls due to the variable implementation time (per EUC). This can take 20 minutes to 30 hours per EUC (depending on the complexity).

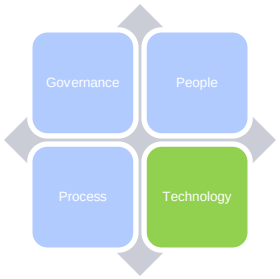
EUC Control Environment - Process



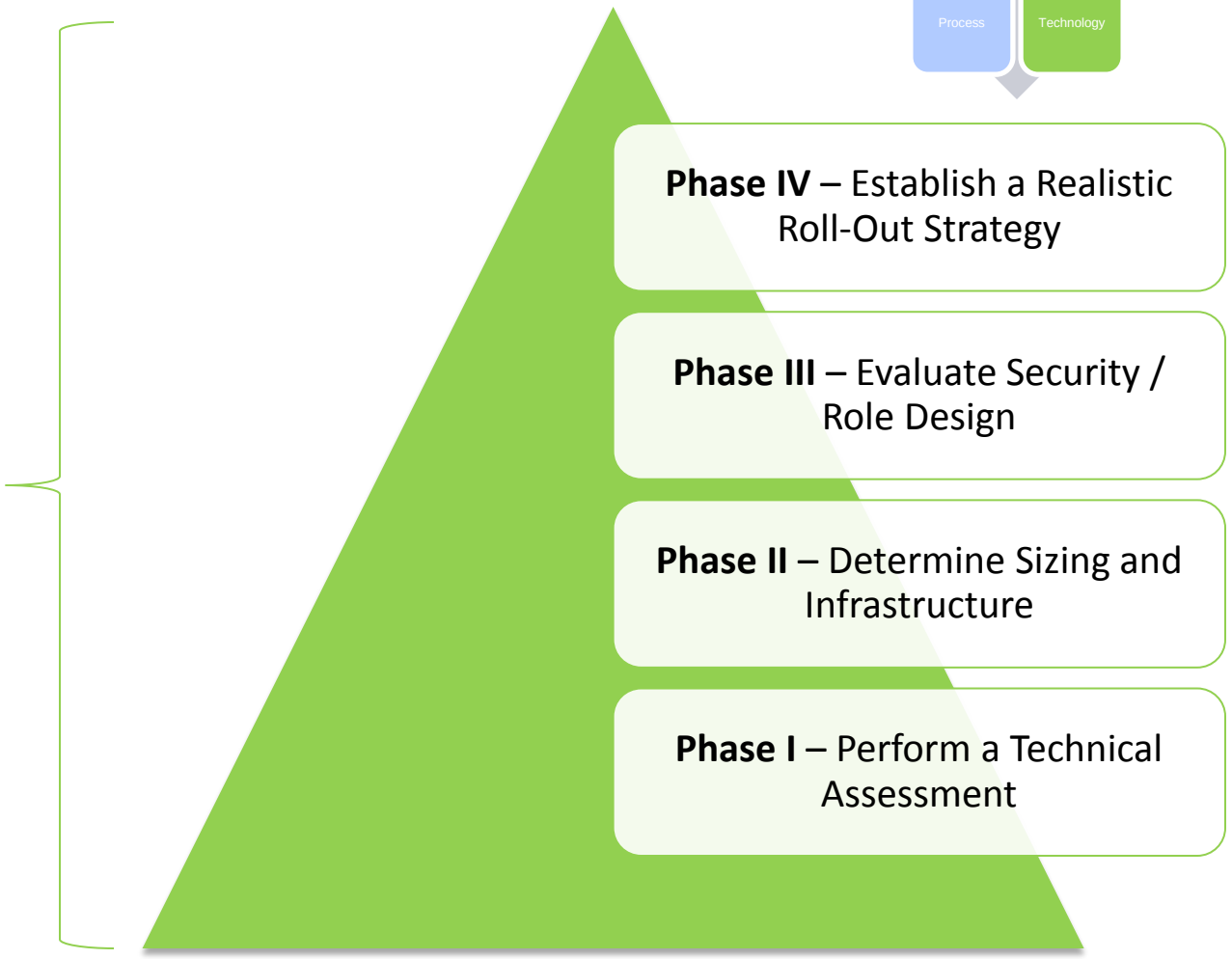
Once management has baselined all high risk EUCs with the new controls, an effective on-going monitoring and governance process should be implemented to ensure that user groups continue to adhere to the defined controls.

Phase V - On-Going Control

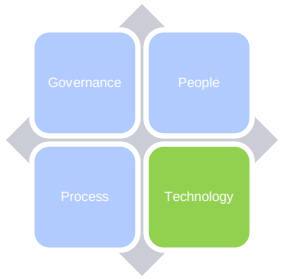
EUC Control Environment - Technology



Throughout the technology selection, implementation, testing process; the other areas of the framework (Governance, People and Process) should be considered and revised as necessary.



EUC Control Environment - Technology



Phase I – Perform a Technical Assessment

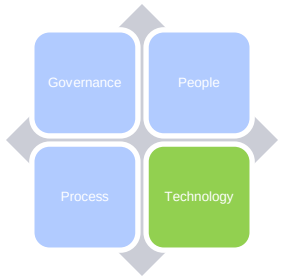
Technology enabler requirements should be defined, and then available options such as manual processes vs. automated tools should be evaluated against the specific technical requirements. Vendor demonstrations and/or pilots should be performed. Existing IT infrastructure should also be considered.

Phase IV – Establish a Realistic Roll-Out Strategy

Phase III – Evaluate Security / Role Design

Phase II – Determine Sizing and Infrastructure

EUC Control Environment - Technology



Phase II – Determine Sizing and Infrastructure

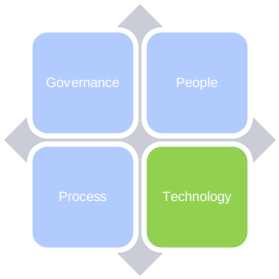
Determine key architecture decisions in the implementation. This may be contingent on strategic decisions made. For Example, if network files shares will be used to secure EUCs, does the current server population have the estimated capacity to accept the additional load? Other considerations may impact this as well. For example, will one enterprise server be used, or will each global region have a separate server for managing EUCs?

Phase IV – Establish a Realistic Roll-Out Strategy

Phase III – Evaluate Security / Role Design

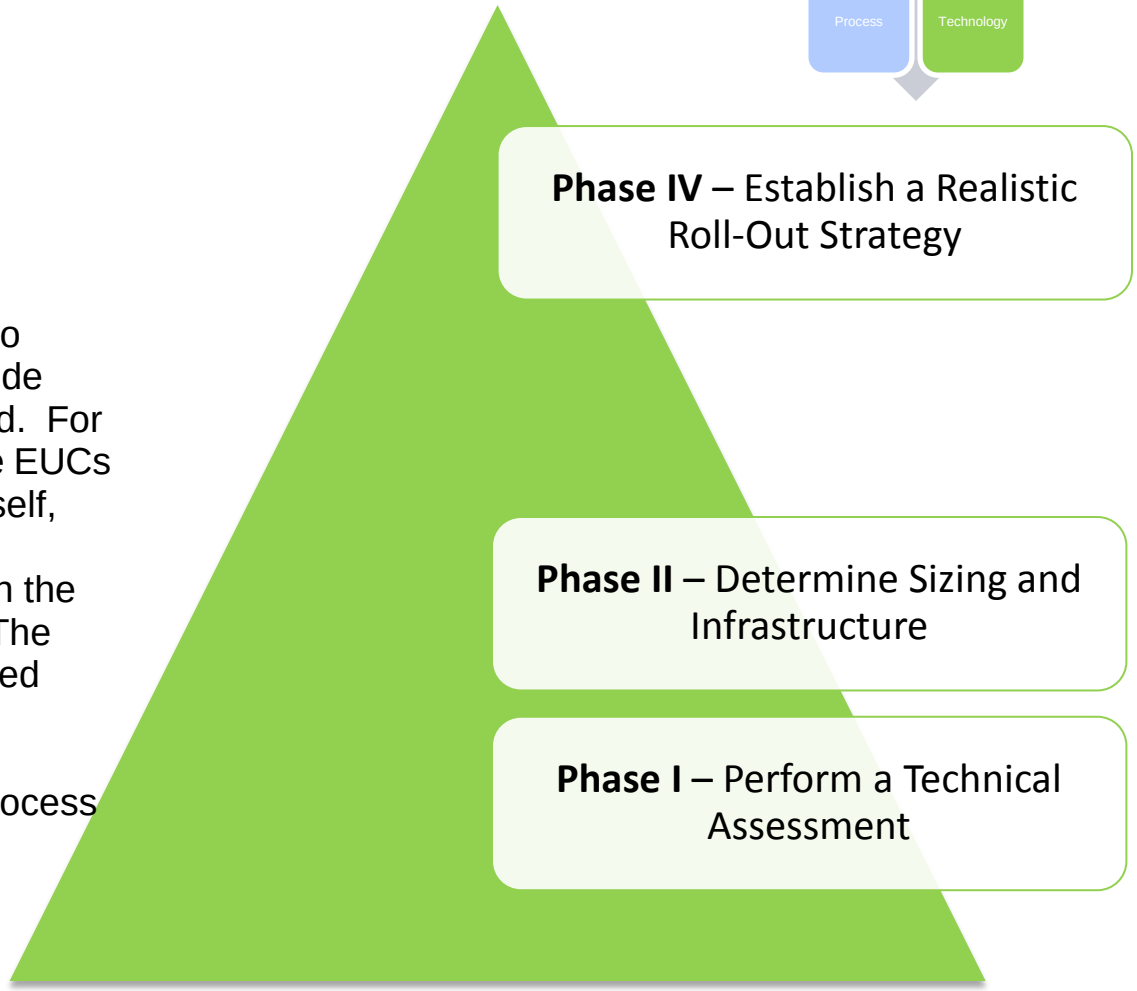
Phase I – Perform a Technical Assessment

EUC Control Environment - Technology

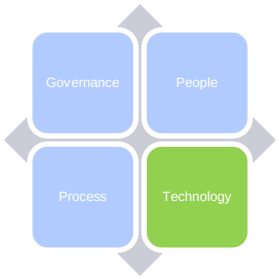


Phase III – Evaluate Security / Role Design

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 vendor tools may allow for controlling different types of access within the EUC, such as read vs. change access. The organization will need to develop a detailed security roles design and configure the technology enablers accordingly. Once established, an on-going maintenance process should be implemented.

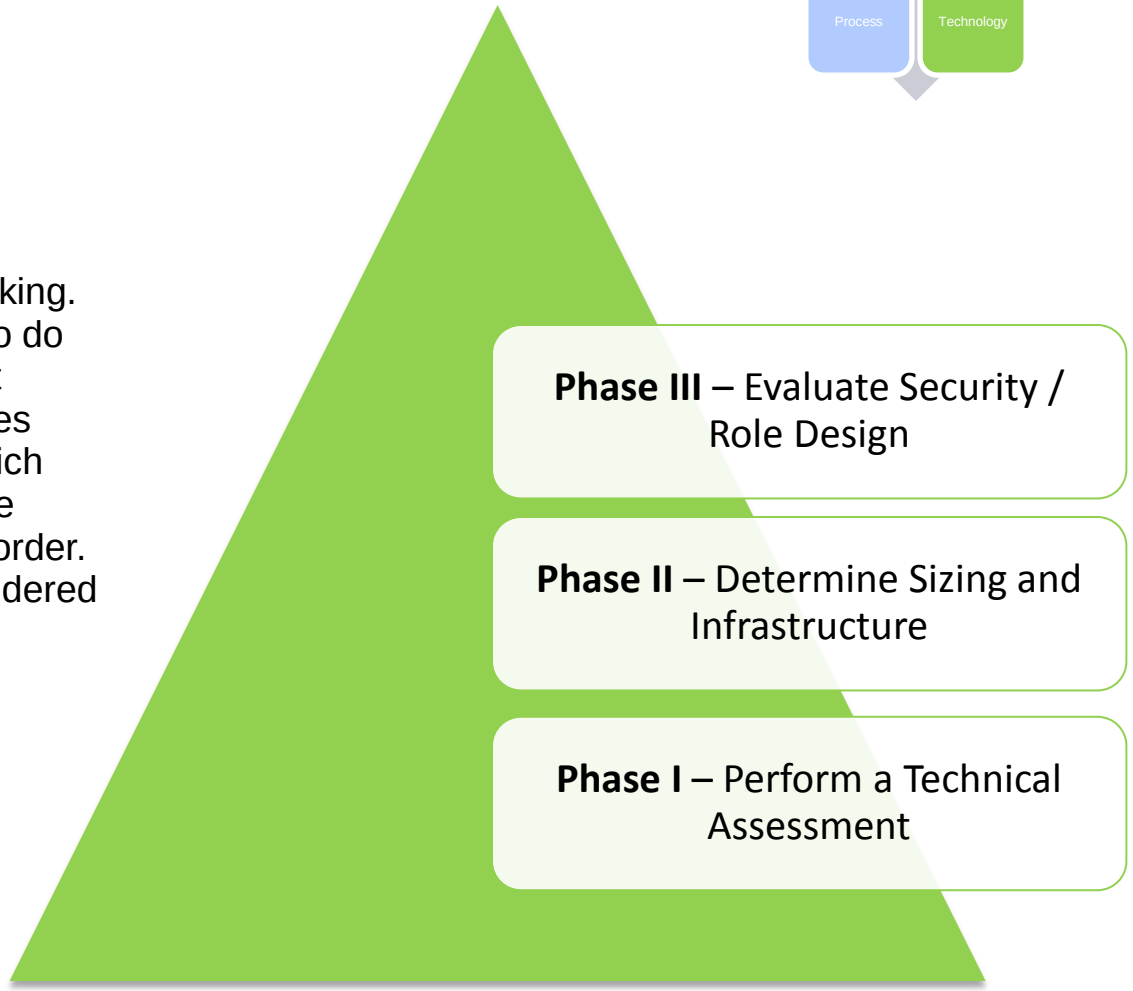


EUC Control Environment - Technology



Phase IV – Establish a Realistic 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.



Summary

- Effective management of EUCs requires a comprehensive program for management and control
- The program should be comprised by elements of governance, people, process and technology
- There is no cookie-cutter solution

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

.