Melinda J. DeCorte, CPA, CFE, CGFM, PMP

Melinda DeCorte has 20 years of accounting, auditing and government financial management experience.

Ms. DeCorte directs, manages and serves in a quality assurance capacity for financial statement audits conducted in accord with government auditing standards. She is experienced in applying applicable Office of Management and Budget, Government Accountability Office (GAO), and American Institute of Certified Public Accountants (AICPA) methodologies and requirements and ensuring that audit teams comply with applicable professional standards. Additionally, she has extensive consulting experience for multiple governmental agencies, primarily focusing on internal controls and risk assessments, financial statement preparation, financial system implementation, and evaluating agencies for audit readiness and compliance with internal control standards and generally accepted accounting principles. Prior to her career in public accounting, Melinda served as a commissioned officer in the United States Army, Finance Corps.

Melinda is a member of the Association of Government Accountants (AGA), the Association of Certified Fraud Examiners, the AICPA and the Texas Society of Certified Public Accountants. She serves as the Vice-Chair of the national AGA Professional Ethics Board and on the advisory council to the GAO in updating the *Standards for Internal Control in the Federal Government* (Green Book). She is currently serving as the President of the Dallas chapter of the AGA and has actively served on multiple committees of the Virginia Society of Certified Public Accountants. She also taught introductory and intermediate-level financial accounting for four years for the University of Virginia, Northern Virginia Center.

Melinda graduated from Georgia State University with a bachelor’s degree in Business Administration (Major in Economics), and completed an additional 30 semester hours in Accounting at the University of Virginia, Northern Virginia Center. She is a Certified Public Accountant (CPA), Certified Government Financial Manager (CGFM), Certified Fraud Examiner (CFE), and Project Management Professional (PMP) and is the Elijah Watts Sells Gold Medal winner with the highest score in the country for the November 2002 Uniform Certified Public Accountant examination.

IT Controls for the non-IT Auditor

May 17, 2018

Association of Government Accountants – Dallas Chapter

Professional Development Training

Session Objectives

What is internal control and why is it so important?

What are the types of information assurance controls?

How do I apply these concepts?

Disclaimer

This session will not prepare you for the CISA exam or qualify you to be an IA auditor

What is internal control?

An integral component of an organization’s management that provides reasonable assurance that the objectives of the organization are being achieved

Objectives and related risks can be broadly classified into three categories:

- Efficient and effective operations
- Reliable reporting
- Compliance with laws and regulations

The plans, methods, policies, and procedures used to fulfill the mission, strategic plan, and objectives of the organization

Fundamental concepts

Geared towards the achievement of objectives

- Operations
- Reporting
- Compliance

A process that is continuously evolving

Effected by the organization's people and the actions they take (or fail to take)

Fundamental concepts (cont.)

Provides reasonable, but not absolute, assurance

Adaptable and flexible

Comprised of the five components working in an integrated manner

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

Why is internal control important?

Helps managers achieve desired results

- Efficient program operations (delivering public services to us – the citizens)
- Effective stewardship of public resources (our taxpayer dollars)

Provides reasonable assurance that the amounts and disclosures reported in the organization's financial statements are materially accurate

- Necessary in achieving a "clean" audit opinion with no reportable internal control deficiencies
- Important in municipal bond ratings (evaluating the credit risk in determining whether to purchase)

OK, but why is internal control really important?

Serves as the first line of defense in safeguarding assets and preventing fraud

- Misappropriation of cash and other assets
- Fraudulent financial reporting (perhaps to cover up misappropriation or to achieve a desired outcome)

Helps to deter public corruption

Avoid embarrassment, public humiliation and ending up on the front page of the newspaper!

ERNST & YOUNG SAYS PENTAGON HAS NO IDEA WHERE $800 MILLION WENT

E&Y discovered that the Defense Logistics Agency “failed to properly document more than $800 million in construction projects,” said Politico*, who also reported this is just one of the many instances where millions of dollars went missing as the accountability system inside the Pentagon is broken.

*POLITICO 02/05/2018

DEFENSE DEPARTMENT SPENT $150 MILLION ON VILLAS, PRIVATE SECURITY GUARDS IN AFGHANISTAN

A report from the SIGAR says the Defense Department's Task Force for Business and Stability Operations paid $150 million for private homes and security guards for U.S. government employees in Afghanistan between 2009 and 2014. Photo provided by a former employee of the TFBSO, shows a villa in Kabul.
*Newsweek 12/3/15

ING

Case Study

Lessons from an $8 million fraud

Background

- ING acquired Mueller’s employer, life insurance company ReliaStar, in 2000.
- As a part of the changeover team, Mueller became an expert on all aspects of the ERP system including financial reporting, journal entries, checks and wire payment processing.
- He was mistakenly given the authority to request and approve checks up to $250,000.
- A co-worker also was accidentally granted the same privileges, while a subordinate was authorized to request checks.
- Mueller, his subordinate, and the co-worker knew each other’s passwords and often logged on as one another to get work done (workaround to accomplish tasks when others were out).
- Mueller realized that he could log on as his co-worker or subordinate and request a check, then log on as himself and approve the check that he had requested.
- Mueller and his subordinate were also allowed to physically pick up checks.

And so the scheme begins…

- Pressured by personal credit card debt, Mueller began to request and approve checks payable to his credit card company.
    - He paid off $88,000 of credit card debt through this method.
- A returned check stopped his spree…for a few months.
- He resumed his scheme, with a slightly more sophisticated method.
    - He set up a company (fake vendor to ING), opened a bank account, and began to issue checks to the company.
    - He coordinated his check issuance days with the days that his subordinate was off, thereby allowing him to pick up the checks.
    - He deposited the checks in the bank account of the fake vendor.
    - He recorded the offsetting expense to ledger accounts that he controlled and that had significant reconciliation activity.
- Mueller told his wife that the extra money was from gambling winnings. After a while, she began to doubt that explanation, and they divorced.

Outcome

- Mueller’s fraud netted nearly $8.5 million in four years (2003 until 2007).
- Mueller bought expensive cars, watches, and nighttime entertainment and paid for numerous trips from Minnesota to Las Vegas.
- The fraud was uncovered when Mueller’s ex-wife expressed her doubts about his income to his co-worker.
- The co-worker then analyzed company records, spotted questionable transactions, and brought them to management’s attention.
- Mueller was sentenced to 97 months in federal prison after pleading guilty to fraud.
- He began his term in February 2009 at the Federal Prison Camp in Duluth, MN, and was released in September 2014.
- Mueller has paid back about $860,000 of the money he stole.
- He now works as Director of Education for a CPA firm, and gives talks on ethics and business crimes

Nathan Mueller Stole $8.5 Million, Served 5½ Years and Says He Emerged Changed Man

"I went into prison thinking my life was over, but it turned out to be a lifesaving and life-changing experience," said convicted fraudster* Nathan Mueller during the closing General Session of the *26th Annual Global Fraud Conference* in Baltimore, Maryland. During his incarceration, he told attendees, he became "the person I always wanted to be."

**The ACFE doesn't compensate convicted fraudsters.*

What can government organizations do?

A study of reported occupational fraud cases in public sector entities published in the *Journal of Government Financial Management** noted the following top three internal control weaknesses:

- Lack of management or independent reviews
- Abuse of authorizations to access cash, other assets or to information systems
- Inadequate level of transaction recordkeeping / documentation

Strong internal control activities and segregation of duties, many of which can be integrated and automated within an organizations' financial management or ERP system can help mitigate the risk of fraud and mismanagement.

*Winter 2014 edition

Control activities

- Control activities are the actions established through policies and procedures that help ensure management directives are carried out
- Control activities help to mitigate risks to achieving the organization’s objectives
- Control activities occur throughout the organization, at all levels and in all functions.
- Control activities include a range of activities:
  - Approvals and Authorizations
  - Verifications and Reconciliations
  - Management reviews of operating performance
  - Physical security of vulnerable assets

Control activities (cont.)

- Segregation of duties is an underlying concept
- Management should divide key duties and responsibilities among different people to reduce the risk of error, misuse, or fraud
  - This includes separating the responsibilities for authorizing transactions, processing and recording them, reviewing/reconciling the transactions, and handling any related assets
- Management should ensure that no one individual controls all key aspects of a transaction or event
- Segregation of duties is typically incorporated into user access controls within a financial management system
  - Depending on the user's assigned role within the system, the user can or cannot process certain transactions or change certain settings

IA Controls – General Controls

Policies and procedures that apply to all or a large segment of an organization’s information systems and help ensure their proper operation

- Security management – framework to manage risk, develop security policies, assign responsibilities, and monitor adequacy of IS controls
- **Access controls** – limit or detect access to IS resources; protect them against unauthorized modification, loss, and disclosure
- **Configuration management** – prevent unauthorized changes to software programs and hardware configurations; assurance that systems are configured and operating as intended
- **Segregation of duties** – manage who can control key aspects of IS operations
- Contingency planning – continue critical operations; protect critical and sensitive data

Access Controls

- Uniquely identify and authenticate users (passwords, tokens, biometrics, key cards, PKI certificates)
- Lockout policy after unsuccessful attempts
- Periodic password changes; password requirements
- Obscure authentication information
- Implement procedures to handle lost, compromised, or damaged authenticators
- Identify authorized users, the access they have, and periodically review for continued appropriateness

Access Controls (cont.)

- Log and review changes to access authorizations
- Remove/disable unnecessary or inactive accounts; remove accounts for terminated individuals
- Limit access to sensitive/privileged accounts
- Limit access to printed/digital media removed from the system to authorized users
- Implement an incident response program
- Log, analyze and follow up on incidents
- Establish adequate physical security over information systems

Configuration Management

- Management reviews and approves planned configuration changes
- Establish a methodology for the design, development, and operation of the system
- Maintain an inventory of hardware and software
- Document a formal change management process
- Management authorizes actual configuration changes

Configuration Management (cont.)

- Document and review detailed specifications of the changes
- Test changes
- Validate that current configuration is accurate, current, and working as intended
- Update software promptly
- Install latest software patches

Segregation of Duties

- Identify and segregate incompatible duties; if limited resources, implement compensating controls such as supervisory review and logging and monitoring
  - This includes roles performed by the systems security manager, system designer, programmer, tester and user
- Key segregations:
  - Data entry and verification of data
  - Data entry and its reconciliation to output
  - Input of transactions for incompatible processing functions (e.g., enter vendor invoices and enter receiving information)
  - Data entry and supervisory approval functions
  - Establish user access based on assigned role within the system

Segregation of Duties (cont.)

- Document job descriptions to reflect assigned duties; employees must understand their responsibilities and segregation of duty principles
- Review access authorizations for incompatible functions
- Monitor staff performance
- Review user activity logs; investigate incompatible and/or unusual actions

IA Controls – Application Controls

Controls over the completeness, accuracy, validity, confidentiality and availability of transactions and data during system processing

- Completeness – all transactions that occurred are input into the system, accepted for processing, processed, and included in output
- Accuracy – transactions are properly recorded, with correct amount/data, and in the proper period; data elements are processed accurately and output is accurate.
- Validity – recorded transactions actually occurred, were properly approved in accordance with management's authorization, and output contains only valid data
- Confidentiality – data and reports and other output are protected against unauthorized access
- Availability – data and reports are available to users when needed

Application Controls (cont.)

- Application level general controls – general controls at the business process application level
- **Business process controls** – automated and/or manual controls applied to business transaction flows
- Interface controls – timely, accurate, and complete processing of information between applications (e.g., feeder system and GL)
- Data management system controls – these controls enforce user authentication/authorization, availability of system privileges, data access privileges, and segregation of duties

Business process controls

- Transaction Data Input – controls over data entering the application (e.g., data validation and edit checks)
- Transaction Data Processing – controls over data integrity within the application (e.g., review of transaction processing logs)
- Transaction Data Output – controls over data output and distribution (e.g., output reconciliation and review)
- Master Data Setup and Maintenance – controls over the key information that is relatively constant and shared between multiple functions or applications (e.g., vendor file).

Business process controls (cont.)

- Document and follow approval procedures for data input
- Use edits to reasonably assure data are valid and recorded in the proper format (detect errors before processing)
- Restrict edit overrides to authorized personnel and regularly review data input restrictions to ensure continued appropriateness
- Processing of input data is automated and standardized
- System entries use transaction logs to reasonably assure that all transactions are processed and identify transactions that were not processed

Business process controls (cont.)

- Transactions with errors are rejected/suspended from processing until the error is corrected
- Reconcile data input with data processed
- Critical output data is reviewed timely
- User access to output data is aligned to user role
- Access to reports is restricted to users with legitimate need
- Master data is regularly reviewed and maintained
- Master data changes are approved (consider segregation of duties)

Limitations

If the organization cannot rely on the general controls over a system, it cannot place reliance on the application level controls within the system!

Limitations

Example:

Application control: System edits that preclude users from entering unreasonably large dollar amounts in a payment processing system

General control: Restriction of unauthorized program modifications that might allow some payments to be exempt from the edit

Case Study

Lessons from an $8 million fraud

General Controls – Access Controls

- Identify and authenticate users
  - In this case, passwords were used, but users shared their passwords with other users
    - Consider the use of multiple authentication techniques – passwords, smart cards, tokens – based on risk
    - Include information security as part of performance management practices

  - Mask passwords during entry, require frequent password changes, require a minimum number and type of characters, require account lock outs after unsuccessful password entry attempts

General Controls – Access Controls

- Authorize users
  - ING did not consider what activities within the system its users could perform, and did not grant/restrict system permissions according to job duties/responsibilities
  - Doing so helps to enforce segregation of duties

- Review and maintain user accounts
  - Although reports were generated, ING did not periodically review access authorization listings for continued appropriateness
  - Access changes should be logged and periodically reviewed
  - Terminate accounts for separated users and/or inactive users
  - Remove unnecessary accounts (default or guest accounts)

General Controls – Segregation of Duties

- Mueller and his co-worker could request and approve high dollar value checks
    - Restrict user access to certain capabilities – ING’s access controls did NOT enforce segregation of duties
    - Employ the use of system roles, aligned with system permissions
    - Review and vet roles and permissions periodically to identify incompatible duties
- Mueller was also able to record free form journal entries (the way he covered up his fraud)
    - Limit the use of free form journal entries and require supervisory review and approval before posting
- ING was not reviewing user activity logs. This may have raised suspicion as to the request and subsequent approval of checks by Mueller, his co-worker and his subordinate.

Application Controls – Business process controls

- Mueller could post transactions to the ledger, and had discretion in choosing the account to which the entry posted
  - Define transaction posting logic for most entries (e.g., based on transaction codes or posting definitions)
  - Minimize the ability to generate free form entries or modify the account to which a transaction can post

- Mueller was able to make changes to master data (set up the fake vendor) without approval
  - ING did not seem to review changes to master data or determine if the changes, especially the creation of new vendors, were appropriate

Correlation to GAO Green Book Principles

Control Environment

GAO Green Book Principles	ING deficiencies in its system of internal control
Principle 2. The oversight body should oversee the entity's internal control system.	• ING did not appear to have an antifraud strategy to deter and detect employee fraud. • At a minimum, fraud awareness training would have alerted Mueller's co-worker that his extravagant lifestyle could be due to fraud.
Principle 4. Management should demonstrate a commitment to recruit, develop and retain competent individuals.	• Mueller's employment with ING was a result of an acquisition, and bypassed any pre-employment screens (past employment verification, background check, credit check) that ING might have had in place.
Principle 5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.	• Individuals were not held accountable for their internal control responsibilities. • AP clerk did not investigate the returned check. • Accountants were sharing passwords.

Risk Assessment

GAO Green Book Principles	ING deficiencies in its system of internal control
Principle 8 – Management should consider the potential for fraud when identifying, analyzing and responding to risks.	• ING did not appear to have performed an assessment of fraud risk.
Principle 9 – Management should identify, analyze, and respond to significant changes that could impact the internal control system.	• ING did not perform an assessment of how the business acquisition impacted the system of internal control.

Control Activities

GAO Green Book Principles	ING deficiencies in its system of internal control
Principle 10 – Management should design control activities to achieve objectives and respond to risks.	• No physical safeguards of assets. • Lack of segregation of duties - individuals should not be able to request checks, approve checks and have access to the checks. • Minimize the ability to generate free form entries or modify the account to which a transaction can post. • Require secondary approval of free form entries (journal vouchers). • Untimely or lack of account reconciliation including research and resolution of variances and management review.

Control Activities - Continued

GAO Green Book Principles	ING deficiencies in its system of internal control
Principle 11 – Management should design the entity’s information system and related control activities to achieve objectives and respond to risks.	• Access controls should be implemented to identify and authenticate users. Although passwords were used, users shared their passwords. • Consider the use of multiple authentication techniques: passwords, smart cards, tokens – based on risk. • Mask passwords during entry, require frequent password changes, require a minimum number and type of characters, and require account lock outs after unsuccessful password entry attempts. • Control user accounts by restricting user access to certain information and capabilities (SoD). • Employ the use of roles, aligned with system permissions. • Security access changes should be logged and periodically reviewed. • Terminate accounts for separated users and/or inactive users. • Changes to master data should be logged and reviewed. • Define transaction posting logic for ledger entries (e.g. based on transaction codes or posting definitions).

Information and Communication

GAO Green Book Principles	ING deficiencies in its system of internal control
Principle 13 – Management should use quality information to achieve the entity's objectives.	• Data analytics could have been performed to identify atypical trends. This may have raised alerts to the fake vendor.
Principle 14 – Management should internally communicate the necessary quality information to achieve the entity's objectives.	• Reports detailing the results of data analysis should be reviewed and distributed to management. • Abnormal interactions with outside parties (e.g. errors, refunds, and overpayments) should be communicated to and reviewed by a risk management person knowledgeable in financial matters.
Principle 15 – Management should externally communicate the necessary quality information to achieve the entity's objectives.	• The AP clerk should have called the credit card company to inquire as to why it returned the check, rather than just send the returned check back to Mueller.

Monitoring

GAO Green Book Principles	ING deficiencies in its system of internal control
Principle 16 – Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.	• ING management was not regularly monitoring roles and permissions within the ERP system and evaluating whether individuals' duties were appropriately segregated. • Reconciliations results were not reviewed.
Principle 17 – Management should remediate identified internal control deficiencies on a timely basis.	• Although an internal company review showed that Mueller and his co-worker had check approval authorities, no further review of transactions appeared to have been conducted.

Additional Resources

Federal Information System Controls Audit Manual (FISCAM): provides a risk-based approach for performing a information system controls audit that is consistent with government auditing standards

Federal Information Processing Standards Publication (FIPS Pub) 199 *Standards for Security Categorization of Federal Information and Information Systems*

FIPS Pub 200*, Minimum Security Requirements for Federal Information and Information Systems*

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*

Speaker Contact Information

Melinda J. DeCorte

CPA, CGFM, CFE, PMP

Direct (703) 725-8559

melindadecorte@gmail.com