VIRGINIA CPA ETHICS
2016 REQUIRED COURSE

ETHICS: GET INVESTED

INSTRUCTOR MANUAL

Virginia Society of Certified Public Accountants

Virginia Society of Certified Public Accountants

Virginia CPA Ethics:

2016 Required Course

Instructor Manual

CPE presentation developed by:
Virginia Society of CPAs (VSCPA)
Jim Cole, CPA
Clare Levison, CPA
Jim Shepherd, CPA

Edited by:
Cheryl Hyder, CPA
Jill Mitchell, CIA
John Riley, CPA
Laura Seal, CPA
Emily Walker, CAE

This training has been created to meet the Virginia Board of Accountancy's (VBOA) annual 2-hour (100-minute) CPE requirement for 2016. In 2003, the Virginia General Assembly passed a regulation requiring all CPAs subject to Virginia CPE requirements to take an annual Ethics CPE course. Each year, the VBOA provides an outline of topics to be included, which can be found at tinyurl.com/2016VBOAEthicsOutline (DOCX). Developed using that outline as the course framework, attendees will be able to accomplish the following fundamental objectives:

- Clarify the impact of VBOA statute changes
- Summarize CPE reciprocity and mobility
- Paraphrase the VBOA policy changes and their effects
- Apply the steps of the AICPA Code of Professional Conduct conceptual framework
- Recall the safeguards and threat assessment and how to employ them in everyday practice
- Understand the CPA's obligation to protect a client or employer's electronic data
- Recognize the importance of compliance with professional standards

The VBOA has confirmed that this class meets the need for 2 hours (100 minutes) of Ethics CPE in Virginia as well as 2 hours of Ethics CPE for CPAs licensed in these other states:

- Maryland: Satisfies 2 hours
- North Carolina: Group study and self study versions satisfy 2 hours for CPAs licensed in Virginia and North Carolina for CPAs who live and primarily work in Virginia
- Washington, D.C.: Satisfies 2 hours
- West Virginia: Satisfies 2 hours

This course may also qualify for similar continuing education credit in other jurisdictions and fulfill Ethics requirements for particular specialized certifications. Attendees are encouraged to consult applicable regulations or regulatory bodies for additional information.

Please note: This class is not intended to be an all-encompassing update or to present all significant events occurring during the prior year. The information provided and scenarios presented do not represent official positions of the VBOA, the American Institute of CPAs (AICPA), the U.S. Internal Revenue Service (IRS), the International Ethics Standards Board for Accountants (IESBA) or any other standard-setting or regulatory body discussed herein, nor do they represent the views of any individual course instructor unless specifically noted. For specific advice or clarification, please research the applicable standards or seek advice from the appropriate governing/regulating organization.

Table of Contents

Virginia-Specific Ethics Course 2016 Outline

A. VBOA Updates — Required discussion.

- Changes to VBOA Statutes effective July 1, 2015
  - Financial Statement Preparation Services
  - Firm Mobility
- CPE Reciprocity/Mobility
- Active — CPE Exempt Status for licensed CPAs
  - Process overview, including pre-approval
- New Virginia-Specific Ethics Course Requirements
  - Board Policy No. 2, Sponsors Providing Continuing Professional Education (CPE)
  - Board Policy No. 4, Continuing Professional Education (CPE) Guidelines

B. General Ethics — Required discussion.

- Ethics Toolkit (Conceptual Framework for Public Practice and Business)
  - Five-step approach to addressing ethical dilemmas
  - Case studies

C. Hot Topics for 2016 — Required discussion.*

- Compliance with Professional Standards
  - Department of Labor (DOL) Report — May 2015
    - Summary (CPA Profession Relevancy)
    - VBOA Responsibilities
    - Case Studies
- Personal Information and Privacy (Data Security)
  - Informing CPAs
  - Professional Responsibilities
  - Case studies
  - Resources

For Virginia-Specific Ethics Course Providers/Instructors

Note: Providers/instructors must provide a copy of this outline to each participant. It is recommended that providers/instructors make cases and other materials available to participants in advance, e.g., by posting them on provider websites.

Important: Virginia-Specific Ethics Course providers/instructors should encourage participants to monitor the VBOA website for updates and information regarding the VBOA. Providers/instructors should also recommend that licensees register with the Virginia Town Hall to receive automated VBOA regulatory updates (townhall.virginia.gov).

***Virginia's Hot Topics for 2016 — Provider/instructor may use discretion as to topic selection from the provided list. Course instruction (topic selections) should be tailored to best suit the audience (private and/or public practice).**

Knowledge Check

1. What is the key to CPE compliance for CPAs licensed in Virginia, whether in public practice or business/industry?

Clarifying language was added to the existing statute to ensure that out of state firms who provide services to Virginia clients meet the same practice monitoring and firm ownership requirements as Virginia-licensed CPA firms.

This change means that all CPA firms providing public accounting services to Virginia clients should be subject to the same requirements, including peer review, regardless of where the CPA firm is licensed.

2. What does the term "principal place of business" mean? How does it relate to CPE reciprocity?

"Principal Place Of Business" — The primary location where a taxpayer's business is performed. The principal place of business is generally where the business's books and records are kept and is often where the head of the firm — or at least upper management — is located.

3. What policy change related to Ethics course sponsors did the VBOA make in 2015?

Sponsors must be approved on an annual basis by the VBOA, and instructors must be licensed and in good standing with the VBOA.

4. What is the key to Active — CPE Exempt status for CPAs licensed in Virginia, whether in public practice or business/industry?

In determining whether a CPA is providing services to an employer in a position that requires the "substantial" use of accounting, financial, tax or other skills, the VBOA has established a working definition of the term "substantial." If a CPA is required to use these skills one or more workdays per month, then the "substantial" test is met and the CPA will not be eligible for Active — CPE Exempt status, meaning the CPA must continue to fulfill all CPE requirements.

Knowledge Check

5. What are the four steps of the AICPA conceptual framework?

1. Identify threats
2. Evaluate the significance of threats
3. Identify safeguards
4. Evaluate the safeguards

6. List five of the top cybercrimes affecting CPAs?

1. Tax refund fraud
2. Corporate account takeover
3. Identity theft
4. Theft of sensitive data
5. Theft of intellectual property

7. What are the six core components of the plan to improve audits?

1. Pre-licensure
2. Standards and Ethics
3. CPA learning and support
4. Peer Review
5. Practice Monitoring of the Future
6. Enforcement

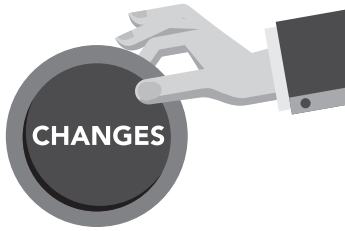
Introduction

Behaving ethically is a lifelong process. It requires a constant effort to apply ethical principles throughout your career, from the formative years through retirement. You're only as ethical as the way you reacted to the last crisis, so invest in ethics. Take it seriously. Don't just put in your two hours to fulfill the requirement for another year. Really put yourself into the course. You get out of it what you put into it.

Rapidly changing technology continues to shape the way CPAs perform their jobs. CPAs need to make an investment in understanding the ethical implications associated with technology, and portions of this course are devoted to the moving target that technological advances create. Technological advances affect the way CPAs communicate with clients and handle their personal information. And while those advances can bring new clients and time-saving process changes to savvy firms and professionals, they also bring threats — from competition to bad actors looking to steal money and personal information. It's important to protect your practice, employer and clients from these kinds of risks and learn what you need to do to capitalize on technological advances while avoiding the pitfalls those advances bring.

Our goal this year is to provide context for a variety of ethical dilemmas you may face in the workplace. From updates on VBOA activities to practical ethics case studies, read on to make your investment in ethics.

Chapter 1:
Changes to Virginia's Accountancy Statutes



Effective July 1, 2015, the accountancy statutes governing Virginia CPAs were changed, through the passage of SB 1125, by clarifying firm mobility for CPA firms and adding a new accounting service.

Firm Mobility

Instructor: In order to set the tone, ask for a show of hands of attendees who hold licenses from jurisdictions other than Virginia. Please make clear to the audience that this section covers mobility for those who hold firm licenses, not individual licenses.

Virginia has long permitted out-of-state CPA firms to provide public accounting services to Virginia clients without having to obtain a Virginia CPA firm license, provided certain criteria are met. Such firms are automatically subject to the enforcement authority of the Virginia Board of Accountancy (VBOA). Clarifying language was added to the existing statute, effective July 2015, to ensure that these firms meet the same practice monitoring and firm ownership requirements as Virginia-licensed CPA firms.

This change means that all CPA firms providing public accounting services to Virginia clients should be subject to the same requirements, including peer review, regardless of where the CPA firm is licensed.

Licensing requirements for firms can be found in the *Code of Virginia*, Section 54.1-4412.1, entitled *Licensing Requirements for Firms*. Two applicable paragraphs of that section read as follows:

A. Only a firm can provide attest services, compilation services or financial statement preparation services to persons or entities located in Virginia. However, this shall not affect the privilege of a person who is not licensed *to include a statement on financial statements indicating that no assurance is provided on the financial statements*, to say that financial statements have been compiled or to use the compilation language, as prescribed by subsections B and C of § 54.1-4401.

B. A firm that provides attest services, compilation *services or financial statement preparation* services to persons or entities located in Virginia shall obtain a Virginia license if the principal place of business in which it provides those services is in Virginia.

C. A firm that is not required to obtain a Virginia license may provide attest services, compilation services, or financial statement preparation services to persons or entities located in Virginia if:
   1. *The firm is licensed in another state, meaning, it can lawfully provide attest services, compilation services or financial statement preparation services to persons or entities in the state where its principal place of business is located; and*
   2. *The firm complies with statutes governing firm practice and firm ownership requirements for Virginia CPA firms and*
   3. The firm's personnel working on the engagement either hold a Virginia license or hold the license of another state which is considered to be substantially equivalent as defined by the VBOA or
   4. The firm's personnel working on the engagement are under the supervision of a person who either holds a Virginia license or holds the license of another state and complies with the substantial equivalency provisions.

These changes place non-Virginia CPA firms under the same statutory requirements as Virginia CPA firms, providing equal footing in the practice of public accounting. This should provide further protection to the public by enhancing quality of services provided by the CPA profession to Virginia's citizens and businesses.

If you have questions about the mobility of your license, visit cpamobility.org.

Knowledge Check:

What is the key to CPE compliance for CPAs licensed in Virginia, whether in public practice or business/industry?

Chapter 1:
Changes to Virginia's Accountancy Statutes

Financial Statement Preparation Services

Effective July 1, 2015, the accountancy statutes governing Virginia CPAs were changed through the passage of SB 1125 by clarifying firm mobility for CPA firms and adding a new accounting service. Both a CPA firm license and peer review registration are required to prepare financial statements for clients in Virginia, without regard to the level of service being provided.

The AICPA issued *Statement on Standards for Accounting and Review Services* (SSARS) No. 21 in 2014. This statement revised professional standards for reviews and compilations and introduced engagements to prepare financial statements as a separate engagement from compilations. These standards are effective for reports issued on or after December 2015, although early adoption is encouraged.

SSARS 21 includes a provision that permits CPAs engaged to prepare a client's financial statements, and not also engaged to perform a compilation, review or audit of those financial statements, to prepare financial statements without actually presenting a compilation report ("Preparation of Financial Statements," Sec. 70). These assignments are not attest services, and as a result, CPAs are not required to make an independence determination. The Virginia accountancy statutes were amended effective July 1, 2015, to clearly include preparation of financial statements as a professional service and ensure consistency with AICPA professional standards. The change makes it clear to both Virginia CPAs and the public that financial statement preparation services are covered in the same manner as audit, review and compilation services.

Under the amended statutes, a firm license is required for CPAs to undertake financial statement preparation services, whether or not the CPAs are providing audits, reviews and compilations. The provision of financial statement preparation services by a firm also requires that firm to enroll in the peer review program.

Virginia's accounting statutes state that only a firm can perform a SSARS 21 Section 70 Engagement to Prepare Financial Statements, and that such a firm must be enrolled in peer review. However, the AICPA peer review program explicitly exempts firms that only perform the preparation of financial statements under SSARS 21 Section 70. Firms licensed in Virginia that perform the preparation of financial statements under SSARS 21 Section 70 as their highest level of service must still enroll in peer review under Virginia law despite the exemption in the Peer Review Program Standards. However, these firms can enroll in an inactive status and will actually not be subject to peer review. Firms otherwise subject to peer review that also perform the preparation of financial statements under SSARS 21 Section 70 will have such engagements included within the scope of their peer reviews.

It is important to note that the amended language does NOT restrict a non-licensee (i.e., a non-CPA) from performing this service. Another notable change is the requirement to obtain a signed engagement letter for SSARS engagements.

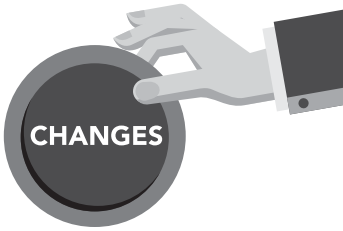
Instructor: Emphasize that CPAs in business or industry who prepare financial statements for their employers are not impacted by this change.

CPE Reciprocity/Mobility

Given the ever-increasing mobility of the American workforce, the issue of CPE reciprocity among substantially equivalent jurisdictions has become a growing concern in the CPA profession. In order to clarify this issue for CPAs providing services in Virginia, on Oct. 5, 2015, the VSCPA and the VBOA jointly issued a letter of explanation to all state board of accountancy executive directors and all state CPA society executive directors.

The letter reads in part:

> Virginia has a longstanding practice of CPE reciprocity for dual and multi-state licensees. The VBOA applies the following practices related to CPE reciprocity:
> - If the licensee's principal place of business is Virginia, then the licensee must comply with Virginia's CPE requirements.
> - If the licensee's principal place of business is in a substantially equivalent jurisdiction and the licensee holds a license of such substantially equivalent jurisdiction, then the licensee may claim a "Home State Exemption" through the CPE Tracking System for Virginia CPE compliance.



The licensee must have an "active" CPA license in good standing in their principal place of business to qualify for the Home State Exemption.

The Virginia-specific Ethics requirement follows a similar pattern, as detailed in the VBOA regulations (emphasis ours):

18VAC5-22-90. Continuing professional education.

A. If during the current calendar year a person who holds a Virginia license provided services to the public using the CPA title, he shall have obtained at least 120 hours of continuing professional education during the three-calendar-year period ending with the current calendar year. For each of the calendar years in that period, he shall have obtained at least 20 hours of continuing professional education, including an ethics course of at least two hours.
   1. If the person also holds the license of another state and Virginia is not the principal place of business in which he provides services to the public using the CPA title, the ethics course taken to comply with this subsection either shall conform with the requirements prescribed by the board **or shall be an ethics course acceptable to the board of accountancy of another state in which the person holds a license**.
   2. Otherwise, the ethics course shall conform with the requirements prescribed by the board.

Instructor: Emphasize that for CPAs, whether in public practice or business/industry, the key to CPE compliance is "principal place of business." CPAs with licenses in other states are encouraged to contact the applicable state boards of accountancy.

CPAs licensed in multiple jurisdictions with Virginia being the principal place of business should check with the individual boards of accountancy where they hold additional licenses with respect to CPE mobility. For example, while the boards in both Washington, D.C., and Maryland allow CPE completed to comply with Virginia's requirement to be used towards their requirements (including the Ethics course), neither provides an exemption from audit/reporting requirements.

Knowledge Check:

What does the term "principal place of business" mean? How does it relate to CPE reciprocity?

Chapter 1:
Changes to Virginia's Accountancy Statutes

Instructor: Note that these cases are handled on a state-by-state basis.

Case Study — Members in Public Practice

Dan Walker, CPA, is a sole practitioner whose residence and principal place of business is in Newburg, Md. Dan has an active Maryland license and also holds an active license in Virginia. Dan's reputation and Internet presence have allowed his firm to attract clients outside of Maryland. He was recently engaged to perform an audit of the financial statements of Skymill, Inc., located in Dahlgren, Va., about eight miles from his office in Newburg. Field work begins on Dec. 12 which follows the week that Dan annually schedules 40 hours of CPE. As Dan sits in the Maryland Ethics class on Dec. 9, he suddenly wonders whether he needs a Virginia-specific Ethics course for his upcoming work in Virginia.

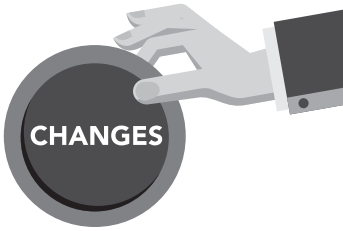
- *Will the Maryland Ethics course be sufficient for meeting his CPE requirements for his Virginia license?*
- *Assuming the same facts as above — except that Dan resides in Maryland, still holds both a Maryland and Virginia license, but his principal place of business (i.e. his practice's office) is in Virginia, next to the Skymill factory — which Ethics course does he need to meet his CPE requirements for his Virginia license?*
- *What if Dan's only CPA license was in Maryland? What are his responsibilities to the VBOA and his new client?*

Instructor: Do not comment on effects on licenses from other jurisdictions. Refer questions to that jurisdiction's Board of Accountancy.

Case Study — Members in Business

Chip Newsom, CPA, resides in Washington, D.C., and is employed full time as the CFO for the American Bankers Association, located in Alexandria. He holds both an active Virginia CPA license and an active District of Columbia license, yet he does not display the certificates, nor has he ever indicated to anyone, in any way, that he holds such licenses. Chip is currently planning his CPE for 2016 and is concerned that he takes the proper Ethics course. As a resident of the District of Columbia, he prefers to take the Ethics course to meet the guidelines of the District.

- *Since Chip is not in public practice, does the District of Columbia's Ethics course also meet Chip's Virginia Ethics CPE requirement?*
- *Assuming the same facts as above, except the Bankers Association relocates to 16th Street in the District of Columbia, will Chip's Ethics requirement change in any way?*
- *What if Chip were only licensed in Virginia?*



Active — CPE Exempt Status

Individuals holding an active CPA license issued by Virginia, but not currently providing services as a CPA or using skills traditionally attributed to accountants, may be eligible for the relatively new Active — CPE Exempt status.

Instructor: Prior to this section, consider asking for a show of hands of anyone who has applied for the CPE Exempt status and see if they will share their experience.

A Virginia CPA is holding out as a CPA and therefore "using the title," without regard to whether or not the individual publicizes their license. Board Regulation 18VAC5-22-40 states: "…holding a Virginia license constitutes using the CPA title." Not disclosing or publicizing — or even actively concealing — one's CPA license will not exempt a licensee from CPE requirements.

Instructor: The VBOA has stated that the above point has generated recurring confusion. Emphasize that whether a licensee fully discloses or "hides" his or her CPA designation is not the deciding factor.

On July 1, 2014, the VBOA implemented the new Active — CPE Exempt status. A CPA who wishes to maintain his or her license, but who is not providing services to an employer or to the public and does not expect to provide such services for a period of time, may apply for the status. The CPE exemption itself is not new, just the requirement to apply for Active — CPE Exempt status in order to take advantage of this exemption. VBOA regulations have specifically allowed for a CPE exemption for certain licensees since at least 2001.

The status is now mandatory before a CPA can cease fulfilling CPE requirements. Previously, a grace period was allowed, but now Virginia CPAs must first obtain approval from the VBOA through a formal application process, including submission of employment information, job description and, if currently employed, information about the employer.

To qualify for the exemption, a licensee must submit a formal application to the VBOA. The application can be found at tinyurl.com/VACPEExempt. Licensees who qualify for this status may continue to use the CPA designation, provided they renew their licenses annually and pay the renewal fee, but will not have to fulfill any CPE requirements.

CPAs who obtain this status may continue to freely use the CPA title and will be allowed to renew their license annually by simply paying the renewal fee without having to obtain any CPE. There is no waiting period prior to applying. A licensee can apply for Active — CPE Exempt status immediately upon a change in working status that could qualify for this status.

A Virginia CPA can only be considered for Active — CPE Exempt status if he or she is not currently providing services to the public or to an employer (i.e. providing to an entity services that require the substantial use of accounting, financial, tax or other skills that are relevant, as determined by the VBOA). Most importantly, the status must be formally requested and approved by the VBOA. Until the Board has formally approved the Active — CPE Exempt status, the CPA is required to fulfill all CPE requirements.

In determining whether a CPA is providing services to an employer in a position that requires the "substantial" use of accounting, financial, tax or other skills, the Board has established a working definition of the term "substantial." If a CPA is required to use these skills one or more workdays per month, then the "substantial" test is met and the CPA will not be eligible for Active — CPE Exempt status, meaning the CPA must continue to fulfill all CPE requirements.

Instructor: The fact that the hurdle of "substantial" has been defined is a critical point to emphasize.

If a CPA obtains the Active — CPE Exempt status, but later begins providing services to an employer or to the public, the CPA is required to immediately notify the VBOA of a change in status. It is very important to note that prior to initiating services to an employer or to the public, the CPA must become CPE compliant for the current reporting cycle.

Retirees who retain an active CPA license cannot simply cease their continuing education without risking sanction, censure, fines and penalties. Any retired Virginia CPA who is not providing services to the public or to an employer must also

Chapter 1:
Changes to Virginia's Accountancy Statutes

apply and be approved for Active — CPE Exempt status before he or she can lawfully stop taking CPE. Alternately, the CPA can voluntarily surrender his or her license.

Instructor: Many classes will include retirees or those contemplating retirement, so this may be a good opportunity to connect with those individuals by emphasizing the above points about retired CPAs.

As of Dec. 31, 2015, the VBOA had processed 1,491 applications for Active — CPE Exempt status and approved 1,025. The examples below, while intended to be instructive, should not be considered as any sort of precedent. Each application is evaluated on its own merits, but the best advice is that any CPA considering this status must contact the VBOA directly for information related to his or her specific situation.

POSSIBLY may obtain CPE Exempt Status:

- Professional dancer
- Medical doctor
- Teacher (non-accounting or financial)
- Retired CPA
- Stay-at-home parent
- CEO of a large company in a non-financial field

UNLIKELY to obtain CPE Exempt Status:

- Accountant
- Chief Financial Officer
- Budget analyst
- Controller
- Tax attorney
- Accounting professor

Instructor: Avoid at all costs using the above examples as precedents. The final decision rests entirely with the VBOA, based on the information (job description, employer information, etc.) provided to the VBOA in the application. For example, a Director of Computing for many industries may be approved as CPE Exempt, but the same title while employed at a bank likely would NOT be approved as CPE Exempt, because the nature of the data involves financial transactions.

Knowledge Check:

What is the key to Active — CPE Exempt status for CPAs licensed in Virginia, whether in public practice or business/industry?

New Virginia-Specific Ethics Course Requirements

In addition to the AICPA Code of Conduct, accounting standards and U.S. Internal Revenue Service (IRS) and state society ethics rules, CPAs in Virginia have an entire hierarchy of legal guidelines, regulatory benchmarks and professional standards with which they must comply. On a day-to-day basis, the policies and regulations of the VBOA may have the most direct impact on many Virginia CPAs. In addition to the Statute changes discussed in this course, the VBOA initiated several changes to its policies during the past year. In order to enhance transparency, the Board has established a practice of introducing any policy change at one meeting of the Board and not acting on the policy change until the next meeting. This allows for possible input from the public and also ensures a more thoughtful process in the consideration of any policy changes.

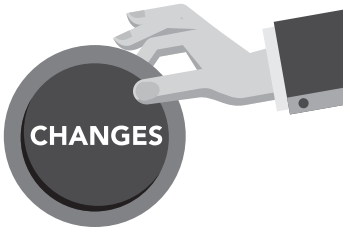
The VBOA instituted two policy changes in 2015 that directly impacted the 2016 Virginia-specific Ethics course.

VBOA Policy No. 2: Sponsors Providing Continuing Professional Education (CPE)

Effective Dec. 11, 2015, the VBOA updated its policy concerning sponsors providing CPE with regard to the annual Virginia-specific Ethics course. Beginning with the 2016 course, the VBOA, through a formal public procurement process, contracted with the VSCPA as the provider of the Virginia-specific Ethics course content and materials.

The following requirements carried over from previous versions of the policy:

- All instructors of the Ethics course must hold an active Virginia CPA license in good standing
- Sponsors desiring to provide the Ethics course must fulfill the following requirements:
  - Obtain the course content and materials from the VSCPA
  - Be preapproved annually by VBOA staff, in writing, as a provider of the course



- Be listed on the VBOA website as a preapproved provider of the course
- Submit all participant comments to the VBOA within 60 days of receipt

- Virginia CPAs will not be granted credit for completing a Virginia-specific Ethics course from a provider that is not approved in advance by the VBOA.

VBOA Policy No. 4: Continuing Professional Education (CPE) Guidelines

Effective June 30, 1015, the VBOA changed its Policy No. 4 related to CPE guidelines. The impact on the Virginia-specific Ethics course is as follows:

New language:

- Through a competitive bid process, the Board contracted with the Virginia Society of CPAs as the only provider of content/material for the Virginia-Specific Ethics Course. The ethics course content/material must follow an annual outline approved by the Board.
- The course must be instructor-led but may be presented in a variety of different formats including, but not limited to, live seminars, conference sessions, online self-study presented by an instructor, live webcast and webcast replays, on-demand webcast and in-house training.

The following language was carried over from previous versions of the policy:

- All licensees providing services to the public or to an employer must complete on an annual basis a Virginia-Specific Ethics Course that complies with Board Regulation 18VAC5-22-90. The two-hour Virginia-Specific Ethics Course is separate and distinct from the one-time American Institute of Certified Public Accountants ethics course needed for initial licensure.
- Virginia licensees must complete the required annual ethics course no later than January 31 of each year to meet the previous calendar-year requirement. Therefore, no sponsor may provide the annual ethics course later than January 31 for the previous calendar year.
- It is the licensee's responsibility to ensure that sponsors providing the Virginia-Specific Ethics Course are listed on the Board's website as an approved provider of this course.
- In order to meet CPE requirements, licensees must also ensure that sponsors provide a certificate of completion or some other form of documentation that includes the sponsor's name, participant's name, course/content name, date taken and CPE hours earned.
- If the licensee is not satisfied with the content of the course or the instructor, the licensee is encouraged to contact the VBOA.
- Licensees will not be granted CPE credit for completing a Virginia-Specific Ethics Course from a non-approved sponsor.

Knowledge Check:

What policy change related to Ethics course sponsors did the VBOA make in 2015?

Instructor: VBOA policies can be changed frequently by the Board. Be sure to monitor the VBOA website to stay up to date on policy changes. Also emphasize that each CPA is responsible for ensuring that they are taking the correct course.

Sources

AICPA. "Statement on Standards for Accounting and Review Services No. 21, Statements on Standards for Accounting and Review Services: Clarification and Recodification." October 2014.

Code of Virginia, Chapter 44: tinyurl.com/6f9ucox

Virginia Board of Accountancy (VBOA) and Virginia Society of CPAs, letter dated Oct. 5, 2015.

Virginia Board of Accountancy. "Accrued Interest." Summer 2015.

Chapter 2:
General Ethics

The CPA license implies objectivity, integrity and sound professional judgment. The public has the expectation that this is what they will be getting when working with CPAs. Along with that expectation come laws, codes, rules, regulations and policies enacted to motivate proper behavior and punish improper behavior on the part of CPAs. At our foundation, we are a profession guided by these laws, and compliance with them is our minimum bar for ethical behavior.

However, the public also has the expectation that we will not only comply with the law but also act in a way that is morally acceptable. Situations may arise that laws, codes, rules, regulations and policies cannot adequately address. There couldn't possibly be a one-size-fits-all solution for every situation, but with the proper toolkit, we can be better equipped to move beyond black and white compliance and navigate the gray area that so often exists when it comes to ethical decision making.

Ethics Toolkit — Conceptual Frameworks for Members in Public Practice and Members in Business

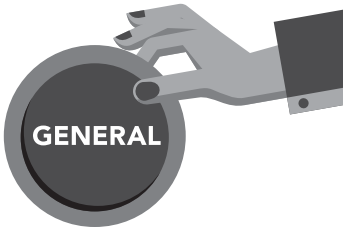
The AICPA provides conceptual frameworks for members in public practice and members in business to apply when assessing their compliance with the Code of Professional Conduct in a particular situation. The conceptual framework approach recognizes that the Code cannot possibly address every conceivable situation and provides a formalized process to apply professional judgment that may be required. The conceptual framework provides guidance on identifying, evaluating and addressing threats to compliance with the rules that results from a relationship or circumstance not otherwise addressed in the Code.

Instructor: A chart of the conceptual framework steps is included in the presentation. Do not discuss the details of each box — they will be discussed in detail as you work through the case studies.

Steps of the Conceptual Framework

The following are the steps of the conceptual framework:

- **Step 1**: Identify threats to compliance with the rules. If no threats, then proceed with service. If threats are identified, proceed to Step 2.
- **Step 2**: Evaluate the significance of the threats to determine whether the threats are at an acceptable level. If threats are at an acceptable level, then proceed with service. If threats are not at an acceptable level, proceed to Step 3.
- **Step 3**: Identify safeguards that can be applied. Safeguards can be existing safeguards or new safeguards.
- **Step 4**: Evaluate the safeguards to determine if they eliminate or reduce threats to an acceptable level. Where you conclude that threats are at an acceptable level after applying safeguards, proceed with service. In some cases, an identified threat may be so significant that no safeguards will eliminate it or reduce it to an acceptable level or you may



be unable to implement effective safeguards. Under such circumstances, providing the specific professional services would compromise your compliance with the rules and you would need to determine whether to decline or discontinue the professional services or resign from the engagement.

The first step is to identify threats. Ask yourself, "Does this relationship or circumstance create a threat to complying with the rules?" If yes, the significance of the threat needs to be evaluated in the second step.

In the second step, evaluate threats. Ask yourself whether or not the threat is at an acceptable level. A threat is at an acceptable level when a reasonable, informed third party who is aware of the relevant information would be expected to conclude that the threat would not compromise compliance with the rules. Consider both qualitative and quantitative factors when evaluating the significance of a threat. If you conclude that a reasonable, informed third party who is aware of the relevant information would be expected to conclude that the threat would not compromise compliance with the rules, then the threat is at an acceptable level and no further evaluation is required. If you conclude that the threat is not at an acceptable level, then you need to proceed to the third step.

The third step is to identify safeguards. Ask yourself what safeguards are in place or could be put in place. When identifying safeguards, remember that one safeguard might eliminate or reduce several threats. However, it might also be necessary to identify several safeguards to eliminate or reduce just one threat. After you have identified new and existing safeguards, proceed to the fourth step.

In the fourth step, evaluate safeguards. Ask yourself if the safeguards eliminate or reduce the threat to an acceptable level. If they do, no further action is required. If they do not, providing the specific professional services would compromise your compliance with the rules and you would need to determine whether to decline or discontinue the professional services or resign from the engagement.

It is important to note that the conceptual framework only applies when no guidance in the Code exists. Failure to use the conceptual framework under those circumstances would constitute a violation of the Code. However, the conceptual framework cannot be used to override existing requirements or prohibitions specifically addressed in the Code.

When the member applies safeguards to eliminate or reduce significant threats to an acceptable level, the member should document the identified threats and safeguards applied. Failure to prepare this documentation would be considered a violation of the "Compliance With Standards Rule."

Conceptual Frameworks for Members in Public Practice and Members in Business

The Code provides conceptual frameworks for members in public practice and members in business that are designed to help members analyze relationships and circumstances applicable to their line of work.

Step 1 of each framework is to identify threats. Many threats fall into one or more of seven broad categories: adverse interest, advocacy, familiarity, management participation, self-interest, self-review and undue influence. Each framework provides definitions and examples of these threats as applicable to members in public practice and members in business.

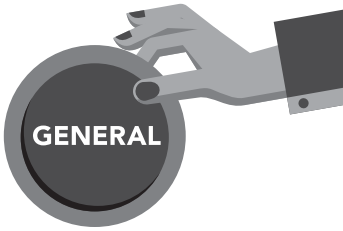
Remember, after you identify threats, you must then evaluate threats, as dictated by Step 2.

Step 3 of each framework is to identify safeguards. Each framework provides categories and examples of these safeguards as applicable to members in public practice and members in business. Categories and selected examples are provided below. You can refer to the Code for the full listing of examples.

Chapter 2:
General Ethics

Definitions and selected examples are provided below. Refer to the Code for the full listing of examples.

	Members in Public Practice	Members in Business
Adverse interest threat	The threat that a member will not act with objectivity because the member's interests are opposed to the client's interests. **Example**: The client has expressed an intention to commence litigation against the member.	The threat that a member will not act with objectivity because the member's interests are opposed to the interests of the employing organization. **Example**: A member has charged or expressed an intention to charge, the employing organization with violations of law.
Advocacy threat	The threat that a member will promote a client's interests or position to the point that his or her objectivity or independence is compromised. **Example**: A member provides forensic accounting services to a client in litigation or a dispute with third parties.	The threat that a member will promote an employing organization's interests or position to the point that his or her objectivity is compromised. **Example**: Obtaining favorable financing or additional capital is dependent upon the information that the member includes in or excludes from, a prospectus, an offering, a business plan, a financing application or a regulatory filing.
Familiarity threat	The threat that, due to a long or close relationship with a client, a member will become too sympathetic to the client's interests or too accepting of the client's work or product. **Example**: A member's immediate family or close relative is employed by the client.	The threat that, due to a long or close relationship with a person or an employing organization, a member will become too sympathetic to their interests or too accepting of the person's work or employing organization's product or service. **Example**: A member uses an immediate family's or a close relative's company as a supplier to the employing organization.
Management participation threat	The threat that a member will take on the role of client management or otherwise assume management responsibilities, which may occur during an engagement to provide non-attest services.	N/A
Self-interest threat	The threat that a member could benefit, financially or otherwise, from an interest in or relationship with, a client or persons associated with the client. **Example**: The member has a financial interest in a client and the outcome of a professional services engagement may affect the fair value of that financial interest.	The threat that a member could benefit, financially or otherwise, from an interest in or relationship with, the employing organization or persons associated with the employing organization. **Example**: A member's immediate family or close relative has a financial interest in the employing organization.
Self-review threat	The threat that a member will not appropriately evaluate the results of a previous judgment made or service performed or supervised by the member or an individual in the member's firm and that the member will rely on that service in forming a judgment as part of another service. **Example**: The member relies on the work product of the member's firm.	The threat that a member will not appropriately evaluate the results of a previous judgment made or service performed or supervised by the member or an individual in the employing organization and that the member will rely on that service in forming a judgment as part of another service. **Example**: When performing an internal audit procedure, an internal auditor accepts work that he or she previously performed in a different position.
Undue influence threat	The threat that a member will subordinate his or her judgment to an individual associated with a client or any relevant third party due to that individual's reputation or expertise, aggressive or dominant personality or attempts to coerce or exercise excessive influence over the member. **Example**: The firm is threatened with dismissal from a client engagement.	The threat that a member will subordinate his or her judgment to that of an individual associated with the employing organization or any relevant third party due to that individual's position, reputation or expertise, aggressive or dominant personality or attempts to coerce or exercise excessive influence over the member. **Example**: A member is pressured to become associated with misleading information.



Members in Public Practice

Safeguards that may eliminate a threat or reduce it to an acceptable level for members in public practice fall into three broad categories:

Safeguards Created by the Profession, Legislation or Regulation

Examples:

- Education and training requirements on independence and ethics rules
- Continuing education requirements on independence and ethics
- Professional standards and the threat of discipline

Safeguards Implemented by the Client *(Note: It is not possible to rely solely on safeguards implemented by the client to eliminate or reduce significant threats to an acceptable level).*

Examples:

- The client has personnel with suitable skill, knowledge or experience who make managerial decisions about the delivery of professional services and makes use of third-party resources for consultation as needed
- The tone at the top emphasizes the client's commitment to fair financial reporting and compliance with the applicable laws, rules, regulations and corporate governance policies
- Policies and procedures are in place to achieve fair financial reporting and compliance with the applicable laws, rules, regulations and corporate governance policies

Safeguards Implemented by the Firm, including policies and procedures to implement professional and regulatory requirements.

Examples:

- Firm leadership that stresses the importance of complying with the rules and the expectation that engagement teams will act in the public interest
- Policies and procedures that are designed to implement and monitor engagement quality control
- Documented policies regarding the identification of threats to compliance with the rules, the evaluation of the significance of those threats and the identification and application of safeguards that can eliminate identified threats or reduce them to an acceptable level

Members in Business

Safeguards that may eliminate a threat or reduce it to an acceptable level for members in business fall into two broad categories:

Safeguards Created by the Profession, Legislation or Regulation

Examples:

- Education and training requirements on ethics and professional responsibilities
- Continuing education requirements on ethics
- Professional standards and the threat of discipline

Safeguards Implemented by the Employing Organization

Examples:

- A tone at the top emphasizing a commitment to fair financial reporting and compliance with applicable laws, rules, regulations and corporate governance policies
- Policies and procedures addressing ethical conduct and compliance with laws, rules and regulations
- Audit committee charter, including independent audit committee members

Remember, after you identify safeguards, you must then evaluate safeguards, as dictated by Step 4.

Independence Conceptual Framework

The code also contains an Independence Conceptual Framework and states:

> "It is impossible to enumerate all relationships or circumstances in which the appearance of independence might be questioned. Thus, in the absence of an independence interpretation that addresses a particular relationship or circumstance, a member should evaluate whether that relationship or circumstance would lead a reasonable and informed third party who is aware of the relevant information to conclude that there is a threat to

Chapter 2:
General Ethics

> either the member's or firm's independence or both, that is not at an acceptable level. When making that evaluation, a member should apply the conceptual framework approach as outlined in this interpretation to analyze independence matters."
>
> "The conceptual framework approach entails identifying threats and evaluating the threat that the member would not be independent or would be perceived by a reasonable and informed third party who is aware of the relevant information as not being independent. The member must eliminate or reduce that threat to an acceptable level to conclude that the member is independent. Threats are at an acceptable level either because of the types of threats and their potential effect or because safeguards have eliminated or reduced the threat, so that a reasonable and informed third party who is aware of the relevant information would perceive that the member's professional judgment is not compromised."

The framework provides definitions and examples of threats as applicable to independence. It also provides categories and examples of safeguards as applicable to independence.

Knowledge Check:

What are the four steps of the AICPA conceptual framework?

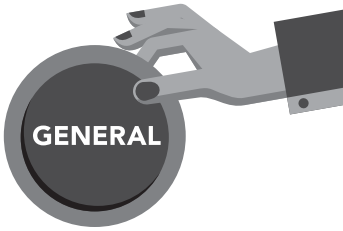
Sources

AICPA Conceptual Framework: tinyurl.com/m3z3cs5

Goria, Ellen. "Revised AICPA Code of Ethics…What's the Fuss?" *Journal of Accountancy*, February 2014: tinyurl.com/o8bw9u8

Goria, Ellen. "User-Friendly AICPA Ethics Code on Horizon." *Journal of Accountancy*, April 17, 2013: tinyurl.com/ljp5ks4

AICPA Ethics Codification PowerPoint, Jan. 24, 2014: tinyurl.com/opgf3kj



Conceptual Framework Case Studies — Members in Public Practice

Case Study No. 1

Robert Romeo, CPA, is completing a year-end audit and discovers that a journal entry was not made which, in his professional judgement, materially affects the presentation of the company's financial statements.

Robert's supervisor, Evan Williams, disagrees and does not want to make the client book the entry, stating that, in his opinion, it was a minor oversight and can be booked in the future reporting period. Who is correct, Robert or Evan?

The issue here is that the auditor's determination of materiality is a matter of professional judgement. Therefore, there is no black and white answer. However, the conceptual framework can be applied to this fact pattern.

Step 1: Identify Threats

Since Robert and his supervisor, Evan, have a difference of opinion relating to the application of accounting principles and auditing standards, Robert identifies that the undue influence threat exists.

Step 2: Evaluate Threats

Since Robert believes the position his supervisor is taking will result in a material misrepresentation, he concludes that the undue influence threat is significant.

Step 3: Identify Safeguards

Robert needs to identify what safeguards could be applied to reduce the undue influence threat to an acceptable level. First, he decides to have additional discussions with Evan about his concerns. The difference of opinion is not resolved after having additional discussions with Evan, so Robert decides to discuss his concerns with Sophia Dabney, Evan's supervisor.

Instructor: What other safeguards could Robert put into place?

Step 4: Evaluate Safeguards

After discussions, Sophia is in agreement with Robert that the client should book the entry. Therefore, Robert believes that the undue influence threat has been reduced to an acceptable level.

To be in compliance with the ethics rules, Robert documents the threat that he identified as being significant and what safeguards he applied.

If Sophia had not been in agreement with Robert, what action should he have considered taking?

Robert should consider:

- Whether the CPA firm's internal policies and procedures have any additional requirements for reporting differences of opinion
- Whether the client's internal policies and procedures have any additional requirements for reporting differences of opinion
- Whether he is responsible for communicating to third parties, such as regulatory authorities or external accountants
- Consulting with legal counsel
- Documenting his understanding of the facts, the accounting principles, auditing standards or other relevant professional standards involved or applicable laws or regulations and the conversations and parties with whom these matters were discussed

If Robert concludes that no safeguards can eliminate or reduce the threats to an acceptable level or that appropriate action was not taken, then he should consider the continuing relationship with his employer and take appropriate steps to eliminate his or her exposure to subordination of judgment.

Instructor: Emphasize that open communication should be a part of the culture at the firm and part of every engagement. Communication can mitigate many issues in situations like this.

Chapter 2:
General Ethics

Case Study No. 2

Jennifer Lambert, CPA, performs non-attest services for XYZ Company. She did an excellent job during the year and, as a result, XYZ Company wants to fly Jennifer to New York City to attend a Broadway show and a dinner, at which she will be given an award for providing XYZ Company with excellent service.

- *Should Jennifer accept the trip to New York City?*

The issue here is that the Code does not contain dollar limitations regarding the point at which objectivity and/or independence might be impaired when accepting gifts or entertainment. Therefore, there is no black-and-white answer. However, the conceptual framework can be applied to this fact pattern.

Step 1: Identify Threats

Since Jennifer is accepting gifts and entertainment from a client, she identifies that the self-interest and undue influence threats exist.

Step 2: Evaluate Threats

Jennifer evaluates the gifts and entertainment to determine if they are reasonable in the circumstances. She considers the following relevant facts and circumstances:

a. The nature of the gift or entertainment
b. The occasion giving rise to the gift or entertainment
c. The cost or value of the gift or entertainment
d. The nature, frequency and value of other gifts and entertainment offered or accepted
e. Whether the entertainment was associated with the active conduct of business directly before, during or after the entertainment
f. Whether other customers or vendors also participated in the entertainment
g. The individuals from the customer or vendor and a member's employer who participated in the entertainment

Since the trip is of significant value, Jennifer concludes that the self-interest and undue-influence threats are significant.

Step 3: Identify Safeguards

Jennifer needs to identify what safeguards could be applied to reduce the threats to an acceptable level. First, she decides that gifts and entertainment from XYZ Company will only be accepted one time per year. Second, she decides that the gifts and entertainment will only be accepted if XYZ Company has a public history of providing similar gifts and entertainment to other service providers.

Instructor: What other safeguards could Jennifer put into place?

Step 4: Evaluate Safeguards

Since this is the only gift and entertainment that XYZ Company has given to Jennifer's firm this year and since the customer service award is something XYZ Company gives out to different service providers each year, Jennifer believes that the self-interest and undue influence threats have been reduced to an acceptable level, so she may accept the trip to New York City.

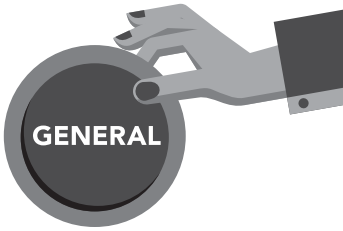
Instructor: Ask the audience if they would accept the trip.

Jennifer documents her evaluation of the threats and safeguards that she identified as being significant and what safeguards she applied.

- *If Jennifer had been performing attest services for XYZ Company, should she accept the trip to New York City to receive a similar award?*

No. When a member on the attest engagement team or in a position to influence the attest engagement accepts a gift from an attest client that is other than clearly insignificant, the risk exists for the client to exercise undue influence over the member (i.e., the "undue influence threat" as defined in the AICPA Conceptual Framework for Independence Standards), possibly resulting in the member being beholden to the client and thereby compromising the member's objectivity and professional skepticism in the performance of the attest engagement.

Since Jennifer concluded that the value of the trip was significant, she determines that there are no safeguards that could be applied to reduce the threats to an acceptable level.



Case Study No. 3

Bobby Bass, CPA, performs attest services for XYZ Company. XYZ Company asks Bobby to help them create some new accounting policies, provide advice on the future strategic direction of the company and decide which recommendations, from an outside consultant that they recently hired, they should implement.

The issue here is that the determination of whether an activity is a management responsibility depends on the circumstances and requires the exercise of judgment.

Step 1: Identify Threats

Since Bobby has been asked to take part in activities that may involve leading and directing an entity, he identifies that the management participation threat exists.

Step 2: Evaluate Threats

Bobby evaluates this threat further and finds that the AICPA Code of Professional Conduct states in Sec. 1.295.030.01:

If a member were to assume a management responsibility for an attest client, the management participation threat would be so significant that no safeguards could reduce the threat to an acceptable level and independence would be impaired.

And in Sec. 1.295.030.02:

Examples of activities that would be considered management responsibilities and, as such, impair independence if performed for an attest client, include:

a. Setting policy or strategic direction for the attest client
b. Directing or accepting responsibility for actions of the attest client's employees except to the extent permitted when using internal auditors to provide assistance for services performed under auditing or attestation standards
c. Authorizing, executing or consummating transactions or otherwise exercising authority on behalf of an attest client or having the authority to do so
d. Preparing source documents, in electronic or other form, that evidence the occurrence of a transaction
e. Having custody of an attest client's assets
f. Deciding which recommendations of the member or other third parties to implement or prioritize
g. Reporting to those charged with governance on behalf of management
h. Serving as an attest client's stock transfer or escrow agent, registrar, general counsel or equivalent
i. Accepting responsibility for the management of an attest client's project
j. Accepting responsibility for the preparation and fair presentation of the attest client's financial statements in accordance with the applicable financial reporting framework
k. Accepting responsibility for designing, implementing or maintaining internal control
l. Performing ongoing evaluations of the attest client's internal control as part of its monitoring activities

In this situation, Bobby would not continue with the steps of the conceptual framework because the situation is directly addressed in the AICPA Code.

It's important to note that it is not possible to specify every activity that is a management responsibility. When the responsibility is not directly addressed in the AICPA Code, the conceptual framework can be applied.

Chapter 2:
General Ethics

Conceptual Framework Case Studies — Members in Business

Case Study No. 1

Robert Romeo, CPA, works for ABC Company, a widget manufacturer. He is going over a list of year-end closing entries and discovers that a journal entry was not made which, in his professional judgement, materially affects the presentation of the company's financial statements. Robert's supervisor, Evan Williams, disagrees and does not want to make the entry, stating that, in his opinion, it was a minor oversight and can be booked in the future reporting period.

- *Who is correct, Robert or Evan?*

The issue here is that the determination of materiality is a matter of professional judgement. Therefore, there is no black-and-white answer. However, the conceptual framework can be applied to this fact pattern.

Step 1: Identify Threats

Since Robert and his supervisor, Evan, have a difference of opinion relating to the application of accounting principles, Robert identifies that the undue influence threat exists.

Step 2: Evaluate Threats

Since Robert believes the position his supervisor is taking will result in a material misrepresentation, he concludes that the undue influence threat is significant.

Step 3: Identify Safeguards

Robert needs to identify what safeguards could be applied to reduce the undue influence threat to an acceptable level. First, he decides to have additional discussions with Evan about his concerns. The difference of opinion is not resolved after having additional discussions with Evan, so Robert decides to discuss his concerns with Sophia Dabney, Evan's supervisor.

Instructor: What other safeguards could Robert put into place?

Step 4: Evaluate Safeguards

After discussions, Sophia is in agreement with Robert that the entry should be booked. Therefore, Robert believes that the undue influence threat has been reduced to an acceptable level.

To be in compliance with the ethics rules, Robert documents the threat that he identified as being significant and what safeguards he applied.

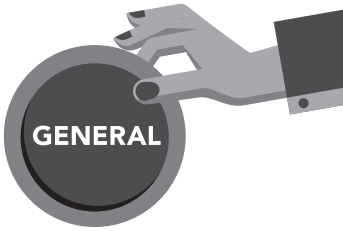
If Sophia had not been in agreement with Robert, what action should he have considered taking?

Robert should consider:

- Whether the organization's internal policies and procedures have any additional requirements for reporting differences of opinion
- Whether he is responsible for communicating to third parties, such as regulatory authorities or external accountants
- Consulting with legal counsel
- Documenting his understanding of the facts, the accounting principles, auditing standards or other relevant professional standards involved or applicable laws or regulations and the conversations and parties with whom these matters were discussed

If Robert concludes that no safeguards can eliminate or reduce the threats to an acceptable level or that appropriate action was not taken, then he should consider the continuing relationship with his employer and take appropriate steps to eliminate his or her exposure to subordination of judgment.

Instructor: Emphasize that open communication should be a part of the culture at the company.



Case Study No. 2

Jennifer Lambert, CPA, is the CFO of ABC Company, which supplies widgets to XYZ Company. ABC did an excellent job during the year and, as a result, XYZ Company wants to fly Jennifer to New York City to attend a Broadway show and a dinner, at which ABC Company will be given an Outstanding Supplier Award.

- *Should Jennifer accept the trip to New York City?*

The issue here is that the Code does not contain dollar limitations regarding the point at which objectivity and/or independence might be impaired when accepting gifts or entertainment. Therefore, there is no black-and-white answer. However, the conceptual framework can be applied to this fact pattern.

Step 1: Identify Threats

Since Jennifer is accepting gifts and entertainment from a customer of her employer, she identifies that the self-interest and undue influence threats exist.

Step 2: Evaluate Threats

Jennifer evaluates the gifts and entertainment to determine if they are reasonable in the circumstances. She considers the following relevant facts and circumstances:

a. The nature of the gift or entertainment
b. The occasion giving rise to the gift or entertainment
c. The cost or value of the gift or entertainment
d. The nature, frequency and value of other gifts and entertainment offered or accepted
e. Whether the entertainment was associated with the active conduct of business directly before, during or after the entertainment
f. Whether other customers or vendors also participated in the entertainment
g. The individuals from the customer or vendor and a member's employer who participated in the entertainment

Since the trip is of significant value, Jennifer concludes that the self-interest threat and undue-influence threats are significant.

Step 3: Identify Safeguards

Jennifer needs to identify what safeguards could be applied to reduce the threats to an acceptable level. First, she decides that gifts and entertainment from XYZ Company will only be accepted one time per year. Second, she decides that the gifts and entertainment will only be accepted if XYZ Company has a public history of providing similar gifts and entertainment to multiple vendors.

Instructor: What other safeguards could Jennifer put into place?

Step 4: Evaluate Safeguards

Since this is the only gift and entertainment that XYZ Company has given to an employee of ABC Company this year and since the Outstanding Supplier Award is something XYZ Company gives to a different supplier each year, Jennifer believes that the self-interest and undue influence threats have been reduced to an acceptable level.

Instructor: Ask the audience if they would accept the trip.

To be in compliance with the ethics rules, Jennifer documents the threat that she identified as being significant and what safeguards she applied.

Chapter 2:
General Ethics

Case Study No. 3

Bobby Bass, CPA, is the Director of Accounting at ABC Company, a widget manufacturer. As a director, he is part of ABC Company's bonus program. ABC Company is looking at revising this program to reduce costs such as the bonus program and has asked Bobby to put together a presentation containing the financial benefits of doing such.

- *How will Bobby ensure that he remains objective when putting together the presentation?*

The conceptual framework can be applied to this fact pattern.

Step 1: Identify Threats

Since Bobby's interests in this situation may be opposed to the interests of his employing organization, he identifies that the adverse interest threat exists.

Step 2: Evaluate Threats

If we assume that Bobby determines that the yearly bonus is of significant value, he concludes that the adverse interest threat is significant.

Step 3: Identify Safeguards

Bobby needs to identify what safeguards could be applied to reduce the threat to an acceptable level. First, he decides that the Accounting Manager will gather and compile the necessary data for the presentation, as he is not part of the bonus program. Second, he decides to involve the Human Resources Manager, who is also not part of the bonus program and asks that she make the presentation with his assistance as needed.

Instructor: What other safeguards could Bobby put into place?

Step 4: Evaluate Safeguards

Bobby believes that once these two safeguards are implemented, the undue influence threat will be reduced to an acceptable level.

Instructor: Ask the audience if they would feel comfortable reporting on the bonus program.

To be in compliance with the ethics rules, Bobby documents the threat that he identified as being significant and what safeguards he applied.

Ethics Pitfalls of Working With Friends

"It is especially ironic when senior teams gather for off-site retreats during which they golf, fly-fish, play tennis and socialize, but during the meetings at those retreats question the need to address friendships on their employee survey." — Rodd Wagner and Jim Harter, from *12: The Elements of Great Managing*

Friendships in the workplace are a natural part of the work environment and often enhance our overall workplace experience. However, workplace friendships can also become a source of ethical dilemmas. How can we best navigate our workplace friendships?

Remember that you're part of a team

It's only natural to be drawn to some people more than others but, at work, everyone needs to feel like part of the team. Make sure your chosen friendships aren't causing other coworkers to feel like outsiders.

Beware of conflicts of interest

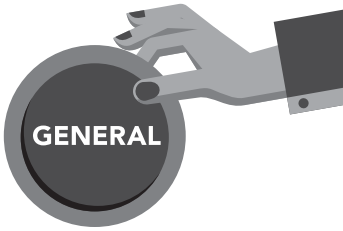
Conflicts of interest can frequently arise when one friend is supervising another. Others may feel that friends will be afforded special treatment. Remember, when dealing with conflicts of interest, be sure that not only is there no conflict in actuality but also that to an outsider it would not appear that your judgement could be biased because of personal friendships.

Keep competition in check

Everyone should give their best in the workplace each day. If your friend's efforts are recognized with a raise or promotion, make sure you're ready to congratulate them rather than becoming envious.

Establish boundaries

Don't let your personal life interfere with your work life and vice versa. Don't bring personal disagreements to work and don't "overshare" information about friends with other co-workers.



Case Study — Members in Public Practice

You are a manager at Clark, Jones & Smith CPA firm and have worked with the CFO of XYZ Company for several years. You have gained a very good working and professional relationship with each other and enjoy going to events and lunches together.

Situation 1

Your CFO friend just got awarded Employee of the Year and the company is paying for her to go to Paris. The CFO is also the 401(k) trustee and fiduciary. The CFO distributes funds out of her account, which she uses as spending money on her trip. The CFO approves her own distribution. This transaction is not within the guidelines of the 401(k) plans as an acceptable disbursement or distribution.

What happens next: You tell the CFO that she's in violation of the plan and that this could have significant implications to the plan if not addressed. She pays it back.

- *Think beyond the legal issues and consider the ethical issues related to your relationship with your friend. What does your intuition tell you about this situation?*

Situation 2

Your CFO friend asks you, as part of the company services your firm provides, to prepare her tax return. You discover that the CFO has not filed her tax return for three years and owes $40,000 in back taxes.

What happens next: You explain to the CFO that this is a fraud risk, because she is the person responsible for the cash activity of the company and she is in financial disarray. You explain that you have a professional responsibility to the owner of the company to bring it to his attention. You give her 24 hours to tell the president on her own. She is nervous and indicates that she is the one who made the decision to hire your firm, not the owner. However, she does tell him and he gives her a loan to pay her taxes.

A CPA engaged by a company can also represent the officers. However, the CPA should be aware that there is a potential for a conflict of interest between the officers and the company. Those interests can be in sync or in conflict. Where such conflicts arise, if the CPA believes they can provide tax preparation services with objectivity, the relationship is disclosed and consent is obtained from both client and employer, they would not be prohibited from providing professional tax services. In addition, the standard engagement typically would be for the current tax year. If an officer has not filed tax returns for three years, that would become a separate additional engagement. Also, if the CFO is a CPA, not filing her own tax returns would be an Act Discreditable under the Code of Professional Conduct.

- *What is the challenge here?*
- *What does your intuition tell you about the actions of the CFO and the owner?*
- *How would your answer change if your friend is or is not a CPA?*
- *What questions would you ask yourself regarding this situation?*
- *Could the conceptual framework be applied to this fact pattern?*

Situation 3

Your CFO friend has asked to get together and wants to invite you, once again, to bid on work for her company.

What happens next: You decline and distance yourself from the individual. You had developed a good friendship, went to lunches together and had your families together. It is all abandoned now.

- *How would you approach making this decision?*
- *What would be an alternative response to abandoning the friendship?*
- *What are your personal moral criteria when it comes to handling the mixture of business and your personal life?*

Chapter 2:
General Ethics

Case Study — Members in Business

You are an internal auditor at XYZ Company and have worked with the CFO of XYZ Company for several years. You have gained a very good working and professional relationship with each other and enjoy going to events and lunches together.

Situation 1

Your CFO friend just got awarded Employee of the Year and the company is paying her to go to Paris. The CFO is also the 401(k) trustee and fiduciary. The CFO distributes funds out of her account, which she uses as spending money on her trip. The CFO approves her own distribution. This transaction is not within the guidelines of the 401(k) plans as an acceptable disbursement or distribution.

What happens next: You tell the CFO that she's in violation of the plan and that this could have significant implications to the plan if not addressed. She pays it back.

- *Think beyond the legal issues and consider the ethical issues related to your relationship with your friend. What does your intuition tell you about this situation?*

Situation 2

Your CFO friend asks you to help her prepare her tax return. You discover that the CFO has not filed her tax return for three years and owes $40,000 in back taxes.

What happens next: You explain to the CFO that this is a fraud risk, because she is the person responsible for the cash activity of XYZ Company and she is in financial disarray. You explain that this situation is putting you in a bad position. You suggest that she tell the president of the company about her failure to file her tax returns and the back taxes that she owes. She is nervous and reminds you that she asked you to assist with the preparation of her return as a personal favor. However, she does tell the president and he gives her a loan to pay her taxes.

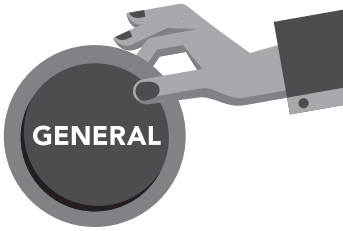
- *What is the challenge here?*
- *What does your intuition tell you about the actions of the CFO and the president?*
- *How would your answer change if your friend is or is not a CPA?*
- *What questions would you ask yourself regarding this situation?*
- *Could the conceptual framework be applied to this fact pattern?*

Situation 3

Your CFO friend has asked to get together and wants to talk about a possible promotion.

What happens next: You decline and distance yourself from the individual. You had developed a good friendship, went to lunches together and had your families together. It is all abandoned now.

- *How would you approach making this decision?*
- *What would be an alternative response to abandoning the friendship?*
- *What are your personal moral criteria when it comes to handling the mixture of business and your personal life?*



Confidential Information in the Age of Social Media

"Who will people decide you are if all they know is what is on your social media page?" — David Bednar

We know that maintaining confidentiality is an important part of cultivating an ethical environment. However, the rise of social media has created even more opportunities for confidentiality to be compromised. How can we ensure that confidential information, as well as our reputation, will be guarded appropriately when we use social media?

Consider your content. Although a post may be intended for a particular audience, you never know where it might show up. Before you put anything in writing, you should consider whether or not you would be willing to have it plastered on a billboard with your face on it.

Be professional. Don't engage in negativity. Never disparage your employer, coworkers, customers or clients on social media.

Don't overshare information about yourself. Be aware of the fact that coworkers, customers and clients might all be reading your posts. If you wouldn't want to share the information with them in a regular conversation, don't share it with them through social media. Social media posts are meant to be personal but not too personal.

Don't overshare information about others. Some things are clearly confidential. Obviously, you shouldn't share things like business plans, pricing structures, etc. However, sometimes oversharing simply boils down to bad manners. Make sure you're aware of both of these pitfalls.

Keep use to a reasonable level. If you're on social media all day, you're indirectly indicating that there isn't much else going on at your place of work. Is that really the message you want to send?

Be honest. Posting information that is fabricated can be just as damaging as posting factual confidential information. If you deem information acceptable to post, make sure it's also accurate.

Case Study No. 1 — Members in Public Practice or Members in Business

A friend sends you a link to a social media discussion from your client's (or employer's) CFO who posted a request for help to reorganize his accounting department. He reveals financial results for his privately-held company in this discussion post.

- *What are the implications of releasing this information on social media?*

Using social media to build relationships and grow a business is a great marketing tool. It is easy, cost-effective and fast. We can reach people all over the world, getting the pulse of what our clients are thinking and building a huge network of referrals and prospects ready to buy our products and services.

However, there are a few risks that go with this powerful tool. One is determining exactly what to share with the public. Another relates to generational issues surrounding the view and usage of social media. As professionals, we deal with confidential client information consistently. The question is: What is confidential and what is public? How we answer this question may in some part be formed by our age, experience and background.

Case Study No. 2 — Members in Public Practice or Members in Business

You overheard a teammate divulging confidential information about your client (or employer) with someone at the coffee shop. This information is potentially damaging to your client (or employer).

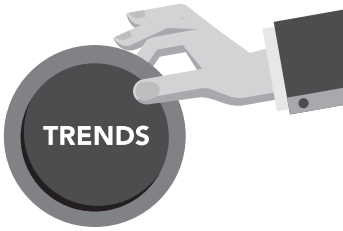
- *What are the ethics issues created by this situation?*

This scenario is a true story, one that happens frequently and takes shape in many forms around the world. Telecommuting is increasing in popularity, with more and more people working out of coffee shops, restaurants, hotel lobbies, airplanes and other public places. As a result, the ethical dilemmas related to confidential client information are growing and the issue of how to protect confidential client (employer) information is becoming more and more urgent to address. While we

recognize that internet threats and hacking into databases is a much bigger issue, the more personal situations like this scenario can be just as devastating. All it takes is one situation like this to cause the loss of a client or employee and create significant impact to our financial results. These circumstances, however, are also more easily preventable and our professional codes of conduct provide guidance on how to reduce the risks occurring from these types of circumstances.

Note: These case studies were made available to us by the National Association of State Boards of Accountancy (NASBA) Center for Public Trust.

Chapter 3:
Trending Topics for 2016



Each year, the VBOA identifies hot topics of current interest to the Board and CPAs. One area of increasing concern to us all and certainly the VBOA is the increasing impact of data breaches, which affect not only CPAs, but businesses and consumers worldwide.

The impact to our profession is great. As data breaches continue to occur, it is very important to be aware of steps CPAs can take to combat this threat.

Personal Information and Privacy (Data Security)

Informing CPAs about Privacy and Personal Information

The adherence to high standards, integrity and confidentiality are marks that define the professionalism of CPAs. One of the hallmarks of our profession is to always maintain client confidentiality and privacy.

A key standard for CPAs to remember is that we must always obtain consent from a client in order to disclose confidential client information. Therefore, it is important to understand what, exactly, constitutes confidential information.

In paragraph .05 of ET section 92, the AICPA Code of Professional Conduct defines confidential client information as follows:

> **Confidential client information**. Any information obtained from the client that is not available to the public. Information that is available to the public includes, but is not limited to, information:
>
> a. in a book, periodical, newspaper or similar publication;
> b. in a client document that has been released by the client to the public or that has otherwise become a matter of public knowledge;
> c. on publicly accessible websites, databases, online discussion forums or other electronic media by which members of the public can access the information;
> d. released or disclosed by the client or other third parties in media interviews, speeches, testimony in a public forum, presentations made at seminars or trade association meetings, panel discussions, earnings press release calls, investor calls, analyst sessions, investor conference presentations or a similar public forum;
> e. maintained by or filed with, regulatory or governmental bodies that is available to the public; or
> f. obtained from other public sources.

Unless the particular client information is available to the public, such information should be considered confidential client information.

Members are advised that federal, state or local statutes, rules or regulations concerning confidentiality of client information may be more restrictive than the requirements in the Code.

Cybersecurity and Client Confidentiality

Imagine entering your office one beautiful morning, and the first thing you receive is a phone call from your technology department informing you that there has been a breach of your company's resources by an outside hacker.

Your first thought is "How could this happen? I thought this only happened to large companies." You continue to assess the situation as you ponder who would do this and what they're planning to do with the data. Finally, you begin to consider your professional responsibilities to the company and your clients.

Obviously, an event like this will ruin your day, but how you act before and after will have an impact on your firm. It is with these thoughts in mind that we should all strive to understand what our ethical duties are in handling and providing confidential data for clients.

What are the top cybercrimes affecting CPAs?

As CPAs, we are often the repository of a wealth of information on our clients, including sensitive financial data. As a result, CPAs may be prime targets for cybercrime.

In October 2013, the AICPA identified the top five cybercrimes encountered by CPA firms:

- Tax refund fraud
- Corporate account takeover
- Identity theft
- Theft of sensitive data
- Theft of intellectual property

Chapter 3:
Trending Topics for 2016

Instructor: A useful flyer from the IRS detailing tax scams is available in the appendices.

It is important to note that most cybercrime is perpetrated by international hackers. In the past, most cybercrime was targeted at large companies and institutions, but thieves have found that it is easier to go after the many soft targets available such as smaller businesses. This is because the amount of money spent on technology defenses is far less than that spent by larger firms.

According to a report from technology firm ExternalIT titled "Financial Firms Face Further Scrutiny of their Cybersecurity — Is Your Firm Ready?", many firms lack:

- Strong password policies and use of two-factor authentication
- Mobile device management
- Device and access monitoring
- Access logs on user access to applications from non-managed devices such as home computers and tablets
- Use of role-based permissions

The cost for cybercrime is increasing globally. According to the ExternalIT report, this cost will exceed $2 trillion globally — 2.2 percent of the IMF's global forecast for the Gross Domestic Product — in 2016.

What are our professional obligations to protect our clients' personal information?

The Gramm-Leach-Bliley Act (GLB) is the main standard that the financial world must follow regarding the protection and privacy of personal information for clients. The GLB Act directed the U.S. Federal Trade Commission (FTC) to establish the Financial Privacy Rule and Safeguards Rule. The FTC Standards for Safeguarding Customer Information Rule (16 CFR Part 314) is the Safeguards Rule that requires financial institutions (that includes CPAs) to ensure the security and confidentiality of customer records and information. The Sarbanes-Oxley Act of 2002 (17 CFR Parts 232 and 249) — Section 404 requirements apply to all U.S. Securities and Exchange Commission (SEC)-reporting companies with a market capitalization in excess of $75 million. It requires financial institutions to develop, implement and maintain an information security program.

To assist its members, the AICPA has developed Generally Accepted Privacy Principles (GAPP), which operationalize the myriad privacy requirements into a single privacy objective that is supported by 10 privacy principles. Each principle is supported by measureable criteria that form the basis for effective management of privacy risk and compliance in an organization.

Instructor: Be sure to differentiate between GAPP and GAAP.

Knowledge Check:

List five of the top cybercrimes affecting CPAs?

AICPA Generally Accepted Privacy Principles

What is privacy?

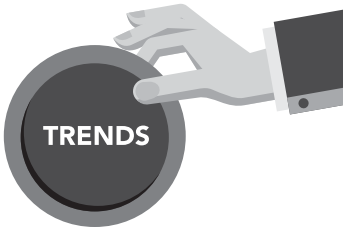
According to the AICPA's GAPP, privacy is defined as "the rights and obligations of individuals and organization with respect to the collection, use, retention, disclosure and disposal of personal information."

Personal information is any information that is about, or can be related to, an identifiable individual. These include prospective, current and former customers, employees and others that the entity has any relationship with. Most information about an individual is considered personal, and some examples given in the Report of Personal Information are:

- Name
- Home and email addresses
- Identification number (i.e. Social Security number)
- Physical characteristics
- Consumer purchase history

The report also lists what is considered Sensitive Personal Information, which generally requires an extra level of care:

- Information on medical of health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions



Unfortunately, GAPP does not define what, exactly, constitutes confidentiality, but the report does indicate examples of what may constitute confidential data:

- Transaction details
- Engineered drawings
- Business plans
- Banking information about businesses
- Inventory availability
- Bid or ask prices
- Price lists
- Legal documents
- Revenue by client and industry

There is not clear guidance as to what constitutes access to this information, so suffice to say, much of this information is considered confidential by agreement or contracts.

Following GAPP

What are steps we can take as CPAs to ensure that we are adhering to privacy principles? The AICPA and the Canadian Institute of Chartered Accountants (CICA) codified GAPP into 10 objectives:

Generally Accepted Privacy Principles (GAPP)

1. **Management**: The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice**: The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. **Choice and consent**: The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. **Collection**: The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention and disposal**: The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retain personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulation and thereafter appropriately disposes of such information.
6. **Access**: The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties**: The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy**: The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality**: The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement**: The entity monitors compliance with its privacy-related complaints and disputes.

A breach occurring in any one of these 10 principles can affect each of us and our practice. As CPAs, we are trusted advisors, and polls rank us as one of the most trusted professions. Confidentiality and professionalism are hallmarks of our profession. That is why a breach can adversely affect us, and why it is so important to embrace an environment of privacy and confidentiality.

Client Privacy Disclosure Under IRC Section 7216

In 2009, new regulations under Sec. 7216 went into effect that impact how CPAs may divulge confidential tax information to third parties for clients. Specifically, this updated U.S. Internal Revenue Code (IRC) section details that a signed consent must be obtained from clients in order to release tax return information to third parties. Even six years after this regulation, it is not uncommon to see practitioners who are unaware of this requirement or of the civil penalties that can be imposed for noncompliance.

In order to provide a framework for complying with Section 7216, visit tinyurl.com/IRCSec7216 to view several versions of the AICPA's 7216 Disclosure, which you may use to adhere to this code section for tax disclosure.

Chapter 3:
Trending Topics for 2016

Some practitioners are under the assumption that having a signed 7216 form will also meet the confidential disclosure requirements for attest or other consulting work. However, a separate disclosure is required to adhere to the AICPA Confidential Client Information Rule for matters beyond tax preparation. Additional consent is required for the release of any confidential information on behalf of a client beyond an IRC Section 7216 disclosure for non-tax information.

Instructors: Please emphasize the following if you have business and industry attendees in your class.

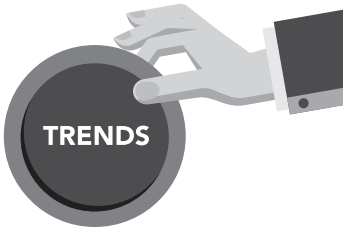
It is also important to note that for members in business, the Code states that a member should maintain confidentiality of his or her employer's confidential information and not use or disclose any confidential employer information obtained as a result of an employment relationship.

Case Study — Public Practice IRC Regulation 7216

Mary, a CPA with the firm of Chihuahua & Labrador, received a call from her longtime client, Collie, who was exasperated trying to complete the final details for a mortgage closing that was to take place the next day for a new home he had purchased. The movers were all set to move his furniture, but the mortgage lender had come back with additional requests for information, without which the closing would be delayed. Collie indicated that he was out of town and did not have access to a fax or printer. Collie requested that Mary send the mortgage company the additional information requested (Latest W-2, paystub and 1040) as she has all his financial information at her office. Mary let him know that she is glad to send copies of these items but will need him to sign a Form 7216 so she can send it to the bank on his behalf. Collie indicates that he cannot get the form, sign it and send it back to her in time but he will have the bank call her to get the information as they have his signed authorization to obtain information on his behalf. Collie indicates to Mary that the bank's "blanket authorization" should provide all the authorization she needs.

- *What are Mary's options at this time?*
- *What steps can Mary take to ensure she is complying with the privacy requirements?*
- *Can Mary send the tax information to the bank and get the forms signed later?*
- *Without Collie's signed 7216 authorization to Mary, what information can Mary disclose to the mortgage lender, if the bank emails her their bank authorization signed by Collie?*

Instructor: Mary can get the form signed and then send tax information via secure email to the bank or she could send via secure email to Collie and Collie can simply forward to the bank without a signed Form 7216. She should realize that disclosure of any information cannot be provided to third parties, including the fact that Collie is a client to the bank, without written authorization. She cannot send the information to the bank and get the forms signed later. The bank's authorization is for the bank and does not provide authority for the disclosure of tax information under Section 7216 by Mary. A specific Form 7216 form must be signed to release tax information to third parties by Mary for Collie.



Case Study — Industry Confidential Disclosure

Mary is a CPA and Chief Financial Officer at Pit Bull Movers, a Virginia company. She received a call from Collie, who heads up sales for Hound Dog Movers in California, requesting confidential information on one of their clients. Collie proposes to Mary that Pit Bull enter into an agreement with Hound Dog so that they can mutually provide moving services for this client which would be a new client for them. Hound Dog would handle the cross-country moving and Pit Bull would handle all local moving.

Collie has been panting over this sale for some time and is eager to iron out the details to get his firms final approval of the terms as well as acceptance of the cost by the new client. He indicates to Mary that it would be helpful to get this deal closed, if Pit Bull Movers could provide any financial, credit and payment history on the company. Collie indicates to Mary that if she would just fax the information over, they could get this deal done and it would be great business for both. Mary lets Collie know that she is glad to consider a joint agreement, but would need to obtain permission from their mutual client to even consider releasing any client information. Collie indicates that this deal is only good if he can get this information quickly. He states that the client needs an answer on whether they can provide services by the end of the week so it is critical this be done quickly.

- *What are Mary's options at this time?*
- *What steps can Mary take to ensure she is complying with the privacy requirements?*
- *Can Mary send the client confidential bank information to the California company and then get her client to sign the forms later?*
- *What are Mary's disclosure obligations if she received a court order subpoena for information for a client?*

Instructor: Mary cannot reveal that the customer is even a customer to Collie until she has the client's permission to do so. She will need to call the client to get the proper authorization for release of information and get her company disclosure authorization forms signed before sending any information at all. She should consult with her company privacy policy and get her own companies confidentiality forms signed before releasing any information or discussing the matter with the California company.

It is probably not possible to accomplish this in a very short timeframe. The short deadline should raise questions as to whether this is a legitimate request or a possible attempt to get client confidential information. Many cybercrimes are the result of employees not following company protocol on privacy. Also, many of the data breaches that occur today are the result of "phishing" and or email scams that allow entrance into a firm by users as compared to a hacker breeching the firewall of a company.

Mary cannot send the information to the other company and get the forms signed later. The law permits disclosure to protect against fraud or in response to a court subpoena or to others who are assuring our compliance with professional standards (e.g. audit).

Chapter 3:
Trending Topics for 2016

Data Breaches

What are our professional responsibilities as CPAs for data security?

Much of the data breaches that occur today are the result of "phishing" and/or email scams, which allow entrance into a firm by users, as opposed to a hacker breaching a company's firewall. As a result, each firm and its individuals should be educated on the steps they should take to safeguard confidential information. This includes procedures in how to best manage passwords and other smart devices to ensure confidentiality of firm assets and clients.

Safeguarding taxpayer data

The following information is taken from IRS Publication 4557, "Safeguarding Taxpayer Data." This guide is to help non-governmental businesses organizations and individuals that receive, maintain, share, transmit or store taxpayers' personal information.

The following safeguards will help you:

- Preserve the integrity of confidential taxpayer data by preventing improper or unauthorized modification or destruction
- Protect the integrity of taxpayer data by preventing improper or unauthorized modification or destruction
- Maintain the availability of taxpayer data by providing timely and reliable access and data recover

Financial institutions as defined by the FTC include tax professionals, data processors and their affiliates and service providers who are significantly engaged in providing financial products or services. They must take the following steps to protect taxpayer information:

- Take responsibility or assign an individual or individuals to be responsible for safeguards
- Assess the risks to taxpayer information in your office, including your operations, physical environment, computer systems and employees, if applicable. Make a list of all the locations where you keep taxpayer information (computers, filing cabinets, bags and boxes taxpayers may bring to you)
- Write a plan of how you will safeguard taxpayer information and put appropriate safeguards in place
- Use on service providers who have policies in place to also maintain an adequate level of information protection defined by the safeguards rule
- Monitor, evaluate and adjust your security program as your business or circumstances change.

Publication 4557 also has the following checklists to help with compliance, which are included in the appendices:

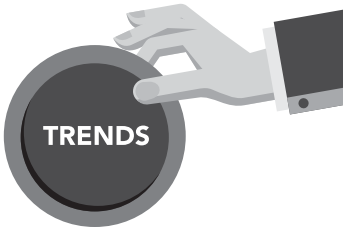
- Administrative Activities
- Facilities Security
- Personnel Security
- Information Systems Security
- Computer Systems Security
- Media Security
- Certifying Information Systems for Use

What do you need to do in the event of a data breach?

The first step you should take if you or your firm fall victim to a data breach is to determine the incident type:

- **Theft**: Unauthorized removal of computers, data/records on computer media or paper files
- **Loss/accident**: Accidental misplacement or loss of computers, data/records on computer media or paper files
- **Unauthorized disclosure/usage**: A person violates disclosure or use policies such as IRC Secs. 6713 and 7216
- **Computer system/network attack**: A virus, Trojan horse or other code-based, malicious entity infects a host and causes a problem such as disclosure of sensitive data or denial of services

After identifying the incident type, follow Publication 4557's recommended actions for incident reporting. Individuals who detect a situation that may be an information security incident should immediately inform the individual designated by the business to be responsible for handling customer information security. The individual responsible for handling customer information security should gather information about the suspected incident.



If you believe the incident compromises a person's identity or their personal information, we recommend you refer to the FTC document, "Information Compromise and the Risk of Identity Theft: Guidance for Your Business." Among other things, this guide will help you determine when to notify local law enforcement, the U.S. Federal Bureau of Investigation (FBI), the U. S. Secret Service, the U.S. Postal Inspection Service, affected business and customers.

Case Study

Jim is a partner in the tax firm Collie, Husky & Shepherd, which has a total of 19 employees. They have prided themselves on embracing technology and staying current on trends. The budget for their Technology line item has increased from 1 percent years ago to 10 percent currently, which is a significant line item for their budget. Jim has refused to allow the firm to use any cloud-based technology solutions due to his view of the "cloud" as a nebulous being that would be easily hacked. As a result, they use only desktop applications, which limits their ability to work from other locations. However, he feels has decreased their ability to be hacked.

- *Is this a good choice for firms to consider?*
- *What are the risks involved in using the cloud?*
- *What are the risks involved in using only desktop applications?*
- *Are smaller firms or larger firms more vulnerable to cyberattacks?*

Instructor: Most cloud providers are equipped to protect user data and allow customers to enjoy economies of scale at minimal expense. That said, no solution is foolproof, and cloud companies must be wary of virtualization risks and any authentication and access control issues that crop up. When using desktop applications only, any disruption to access to those applications would disrupt service to clients, and this policy would not mitigate the risk that comes with employees allowing access to systems.

Speaking broadly, smaller businesses are among the most vulnerable to Internet crime because of their unstructured approach to online security and an increased focus from thieves on smaller firms.

Audit Quality

Instructor: The 2015 report issued by the DOL and EBSA concluded that employee benefit plan (EBP) audit quality has not improved since their last assessment, with nearly four of every 10 audits containing deficiencies. The report found that the smaller the firm's employee benefit plan audit practice, the greater the incidence of audit deficiencies.

The U.S. Department of Labor (DOL) has been presenting across the country the conclusions of a report issued in May 2015 entitled "Assessing the Quality of Employee Benefit Plan Audits". Since the report did not contain good news for the CPA, its findings are an area of emphasis for the DOL, its Employee Benefits Security Administration (EBSA) and the AICPA.

The EBSA review was intended to assess the level of quality of audit work performed by independent qualified public accountants. The agency reviewed Form 5500 Annual Return/ Report filings and related audit reports for the 2011 filing year, consisting of 81,162 filings that contained CPA audit reports. Those audits were performed by 7,330 different CPA firms. Historically, EBSA has found that CPAs with smaller employee benefit plan (EBP) audit practices have had the most audit deficiencies, so the agency divided the population of CPAs into six strata based on the number of plan audits a firm performed.

Findings

The EBSA found that 61 percent of the audits across all strata fully complied with professional auditing standards and had only minor deficiencies under professional standards. However, 39 percent of the audits contained major deficiencies with respect to one or more relevant U.S. Generally Accepted Auditing Standards (GAAS) requirements, which would lead to a rejection of a Form 5500 filing, putting $653 billion and 22.5 million plan participants and beneficiaries at risk.

The review found a clear link between the number of EBP audits performed by a CPA and the quality of work performed. CPAs who performed the fewest number of employee benefit plan audits annually had a deficiency rate of 76 percent. In contrast, the firms performing the most plan audits had a deficiency rate of only 12 percent.

Chapter 3:
Trending Topics for 2016

The accounting profession's peer review and practice monitoring efforts have not resulted in improved audit quality or improved identification of deficient audit engagements. In four of six audit strata, a substantial number of CPA firms received an acceptable peer review report, yet had major deficiencies in the audit work that the EBSA reviewed.

CPA firms that were members of the AICPA's Employee Benefit Plan Audit Quality Center (EBPAQC) tended to produce audits that have fewer audit deficiencies. Most CPA firms in the two smallest audit strata were not EBPAQC members.

Training specifically targeted at audits of employee benefit plans may contribute to better audit work.

Of the 400 plan audit reports reviewed, 67 (17 percent) of the audit reports failed to comply with one or more of the Employee Retirement Income Security Act's (ERISA) reporting and disclosure requirements.

Recommendations of the report include:

Enforcement

- Enforcement to focus on smaller CPA firm employee benefit audit practices
- Work with NASBA and the AICPA to improve the investigation and sanctioning processes
- Amend ERISA to make sure the annual reporting civil penalties focus on the responsible party
- Work with AICPA Peer Review staff to streamline and improve the peer review process and identify those CPAs who have not received an acceptable peer review for further referral to state Boards of Accountancy

Instructor: The included video will summarize the main points of the DOL report. Instructors should be familiar with the content of the video in case the video does not work.

Regulatory/Legislative

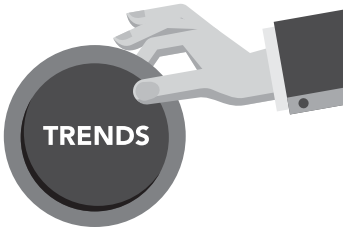
- Amend the definition in ERISA of "qualified public accountant" to include additional requirements and qualifications necessary to ensure the quality of plan audits
- Amend ERISA to repeal the limited-scope audit exemption. When auditors have to issue a formal and unqualified opinion, they have a powerful incentive to rigorously adhere to professional standards that their opinion can withstand scrutiny. The limited-scope audit exemption undermines this incentive by removing auditors' obligations to stand behind the plans' financial statements.
- Amend ERISA to give the U.S. Secretary of Labor the authority to establish accounting principles and audit standards that would protect the integrity of employee benefit plans and the benefit security of participants and beneficiaries

Outreach

- Work with NASBA to encourage state boards of accountancy to require specific licensing for CPAs who perform employee benefit plan audits
- Continue and expand EBSA's outreach activities
- Communicate with state boards of accountancy regarding the results of the study and the need to ensure that only competent CPAs are performing benefit plan audits
- Expand ESBA's outreach with individual state societies of CPAs who have large number of plan audits performed by CPA firms in the 1–5 plan audit stratum

The AICPA EBPAQC issued the Firm Best Practices in its brochure, "Performing Quality ERISA Employee Benefit Plan Audits: Firm Best Practices."

- ***Leadership responsibilities for quality within the firm*** — *The firm should promote an internal culture based on the recognition that quality is essential in performing engagements and should establish policies and procedures to support that culture.*
- ***Relevant ethical requirements*** — *The firm should establish policies and procedures designed to provide it with reasonable assurance that the firm and its personnel comply with relevant ethical requirements. The AICPA Code of Professional Conduct established the fundamental principles of professional ethics, which include:*
  - *Responsibilities*
  - *The public interest*
  - *Integrity*
  - *Objectivity and independence*



- *Due care*
- *Scope and nature of services*

- ***Acceptance and Continuance of Clients and Engagements** — The firm should establish policies and procedures for the acceptance and continuance of client relationships and specific engagements, designed to provide the firms with reasonable assurance that it will undertake or continue relationship and engagements only where the firm:*
  - *Has considered the integrity of the client, including the identity and business reputation of the client's principal owners, key management, related parties and those charged with its governance and the risks associated with providing professional services in the particular circumstances;*
  - *Is competent to perform the engagement and has the capabilities and resources to do so; and*
  - *Can comply with legal and ethical requirements*

The firm should obtain such information as it considers necessary in the circumstances before accepting an engagement with a new client, when deciding whether to continue an existing engagement and which considering acceptance of a new engagement with an existing client.

- ***Human Resources** — The firm should establish policies and procedures designed to provide it with reasonable assurance that it has sufficient personnel with the capabilities, competence and commitment to ethical principles necessary to:*
  - *Perform its engagements in accordance with professional standards and regulatory and legal requirements and*
  - *Enable the form to issue reports that are appropriate in the circumstances.*

  Such policies and procedures should address the following:
  - *Recruitment and hiring, if applicable;*
  - *Determining capabilities and competencies;*
  - *Assigning personnel to engagement, if applicable;*
  - *Professional development; and*
  - *Performance evaluation, compensation and advancement*
- ***Engagement Performance** — The firm should establish policies and procedures designed to provide it with reasonable assurance that engagements are consistently performed in accordance with professional standards and regulatory and legal requirements and that the firm or the engagement partner issues reports that are appropriate in the circumstances. Required policies and procedures should address:*
  - *Engagement performance,*
  - *Supervision responsibilities and*
  - *Review responsibilities*
- ***Monitoring** — The firm should establish policies and procedures designed to provide the firm and its engagement partners with reasonable assurance that the policies and procedures relating to the system of quality control are relevant, adequate, operating effectively and complied with in practice. Such policies and procedures should:*
  - *Include an ongoing consideration and evaluation of the firm's system of quality control to determine*
    - *The appropriateness of the design and*
    - *The effectiveness of the operation of the system of quality control.*
  - *Assign responsibility for the monitoring process to a partner or partners or other persons with sufficient and appropriate experience and authority in the firm to assume that responsibility.*
  - *Assign performance of monitoring of the firm's system of quality control to qualified individuals.*
  - *The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of:*
  - *Adherence to professional standards and regulatory and legal requirements;*
  - *Whether the quality control system has been appropriately designed and effectively implemented; and*
  - *Whether the firm's quality control policies and procedures have been operating effectively, so that reports that are issued by the firm are appropriate in the circumstances.*

The AICPA and the VSCPA, as well as other state societies, have joined forces to provide resources and guidance to CPAs who are performing audits in this area. On the state level, the VSCPA is committed to supporting regulation of Virginia CPAs that will help ensure the highest standard of audit quality. The VSCPA is confident in the steps already underway and in the works that address quality issues and ask

Chapter 3:
Trending Topics for 2016

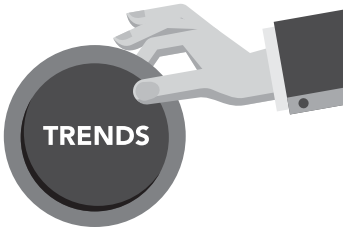
you, as the Society's members, colleagues and stakeholders, to wholeheartedly join in this effort. There are vast resources now available to assist in the area of EBP audits.

Case Study No. 1

John is with the firm of Smith, Thane & Lame in a small town in rural Virginia. John recently made partner and one of his duties as partner is to audit the EBP for one of the firm's larger clients' Mercantile and Merchants Department Store, which just recently hired its 100th employee. While John is an excellent auditor, he has never performed an employee benefit audit and the firm does not belong to an audit quality group.

- *What is the auditor's objective in performing an EBP audit for Mercantile and Merchants?*
- *Does an EBP audit assure compliance with ERISA?*
- *What is John's responsibility to the client for an EBP audit?*
- *Can the firm begin this engagement without any additional training?*
- *What steps could he take to help ensure that this audit does not have deficiencies?*

Instructor: ERISA contains a requirement for annual audits of plan financial statements by an independent, qualified public accountant. Generally, plans with 100 or more participants are subject to the audit requirement, which is intended to ensure the integrity of financial information incorporated in the annual reports. Although the audit requirement in ERISA is an important part of the total process designed to protect plan participants, a U.S. GAAS audit is not designed to ensure compliance with ERISA. Under the law, plan administrators, the IRS and the DOL each have responsibility to ensure such compliance.



The independent auditor's objective and responsibility under U.S. GAAS is to express an opinion on whether the financial statements are fairly presented in conformity with U.S. GAAP, and that the related supplemental information is presented fairly, in all material respects, when considered in conjunction with the financial statements taken as a whole.

The firm cannot begin the engagement without additional training. The Designated Partner is responsible for confirming that there is a partner in the firm who has the necessary training and education to understand specific audit procedures and reporting requirements for all types of EBP audits that the firm performs. Only someone with the appropriate background can determine that enough time is allocated to these audits so that economic considerations do not override the time required to comply with all requirements in the professional standards with due professional care. To ensure that the audit does not have deficiencies, John can become a member of the AICPA's Employee Benefit Plan Audit Quality Center and adhere to firm best practices.

Case Study No. 2

Mary is with the firm of Beagle & Norwich in the Northern Virginia area. Mary's largest client (Maine Chow) has asked her to include in their audit for the firm an audit for the employee benefit plan as they are required to have the audit this year. Jim, the President of Maine Chow, has indicated to the auditor that he considers this audit a compliance nuisance and that he is not expecting this to be much of a cost increase over his current audit fee, as they have not budgeted for it. He says, "After all, it is just an audit of the retirement plan, and they only use low-cost index funds as the investments." Jim says he is fine paying the going rate for the audit of his company but he expects a significantly reduced fee on the Employee Benefit audit. Mary does not want to lose Maine Chow as an audit client and indicates that she will ponder the matter and quickly suggests that perhaps she can get one of her less experienced auditors to perform the employee benefit audit.

- *Are there any fiduciary issues with Jim's statements regarding the retirement plan and ERISA?*
- *Can Mary perform this audit?*
- *How should Mary handle this situation with Maine Chow?*

Instructor: The independent auditor's objective and responsibility under U.S. GAAS are to express an opinion on whether the financial statements are fairly presented in conformity with generally accepted accounting principles, and that the related supplemental information is presented fairly, in all material respects, when considered in conjunction with the financial statements taken as a whole. Maine Chow's plan administrator has a fiduciary requirement to the plan and its participants which means that the administrator must manage the retirement plan for the exclusive benefit of plan participants.

Mary can potentially perform the audit if the proper requirements (personnel and otherwise) are met under professional standards. She should go over the EBP audit requirements with Maine Chow's plan administrator and indicate that they have to adhere to professional standards or they cannot do the audit, and while there is a cost to the plan for the audit, they cannot shortcut the audit and be in compliance.

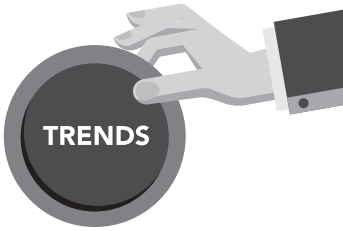
Chapter 3:
Trending Topics for 2016

Public Company Audit Quality

In a November interview with Accounting Today reporter Daniel Hood, U.S. Securities and Exchange Commission (SEC) Chief Accountant James Schnurr said, "Overall, I think audit quality is getting better, but there's room for improvement and it's important that firms stay committed to continuing to improve." This is good news in contrast to the recent issues with EBP audits, and audit quality remains a primary focus of CPAs and professional societies across the country.

The AICPA's Center for Audit Quality (CAQ) has also followed the issue and released a report on general audit quality, "CAQ Approach to Audit Quality Indicators," in April 2014. The following excerpt discusses the value of audit quality indicators (AQI) in providing insight into a firm's practices and systems.

> Audit firms are required to establish a system of quality control that complies with regulatory and legal requirements and that ensures audit reports issued by the firm are appropriate. An audit firm's system of quality control is intended to address certain key elements, such as independence, integrity, objectivity, personnel management (which includes sufficiency of resources, technical knowledge and experience), engagement performance, communication and reporting and monitoring.
>
> The CAQ believes a set of potential AQI could provide additional perspective on the key elements of a firm's system of quality control as it applies to a particular audit and could be useful to further an audit committee's understanding of matters that may contribute to the performance of a quality audit. For instance, a set of AQI could promote robust discussions about an audit firm's ability to support and perform quality audits. They may also assist audit committees in better understanding the audit firm's policies, procedures and processes related to its system of quality control. Additionally, a set of AQI may provide audit committees insight into the engagement team's performance. A set of AQI may also assist audit committees in better understanding the risks to audit quality that may exist on the audit, which could allow for more robust discussions about the audit firm's plan to manage such risks. However, due to the nature and number of inputs that can impact the quality of an audit, no single metric should be viewed as having a causal relationship to audit quality. Nevertheless, we believe a set of indicators, taken as a whole, may provide those overseeing the audit with information and additional transparency into the systems and processes that underlie the performance of an audit.
>
> In identifying potential AQI for this purpose, we believe it is important to consider the following thematic elements of audit quality, which were developed with consideration of perspectives provided by various standard-setters around the world, and are based upon the key elements discussed above. Therefore we believe they facilitate the identification of matters that are most relevant to an audit committee's oversight responsibilities.
>
> #### CAQ Approach to Audit Quality Indicators
>
> 1. **Firm Leadership and Tone at the Top** — The audit firm's leadership, through its tone at the top, emphasizes the importance of audit quality, adherence to professional standards, independence and objectivity and holds itself accountable for the effectiveness of the audit firm's system of quality control.
> 2. **Engagement Team Knowledge, Experience and Workload** — Professional staff are knowledgeable, experienced and have sufficient time to perform quality audits.
> 3. **Monitoring** — Processes and controls are in place to assess audit engagement performance and the sufficiency of the audit firm's system of quality control and make any necessary changes.
> 4. **Auditor Reporting** — Reports are reliable, useful and timely; auditor communications are effective.
>
> Further, AQI, like most evaluative data, are most effective when accompanied by a robust discussion (written or oral). Without these discussions, there is a risk that an AQI or changes in an AQI over time, may not tell a complete story or could be misleading. For example, the fact that an engagement team is experiencing higher than expected overtime could reflect that they have encountered an



unforeseen issue and are spending extra time in order to maintain high audit quality. Alternatively, it could mean that the team is overburdened, which could have an impact on audit quality. As a result, it is important to provide the appropriate context when communicating AQI.

In May 2015, the AICPA issued its six-point plan to improve audit quality. The plan states, "For the past couple of years, audit quality has surfaced as a focus around the globe, for both public and private companies. In early 2014, the AICPA decided a broader, bolder step than ever before was needed to bring solutions to the auditing challenges for private companies."

The centerpiece of the plan was the six points aimed at improving audits:

Pre-licensure
Next version of CPA Exam is designed to increase assessment of higher-order skills, such as critical thinking and professional skepticism; high school AP accounting course; changes to college-level accounting education; additional doctoral-level audit professors with practical experience

Standards and Ethics
Quality control standards implementation support; evaluation of clarified standards implementation; auditor's report revisions; ethics code codification**CPA Learning and Support**
Competency models for audits, including employee benefit plan and governmental, competency assessment tools, targeted resources to develop competencies; certificate programs to demonstrate competence; nano, blended and informal learning programs

Employee Benefit Plan and Governmental Audit Quality Centers' resources, tools and training; Center for Plain English Accounting; audit guides, risk alerts and practice aids

Peer Review
Focus on greater risk industries/areas, including EBP and Single Audits; more significant remediation including pre-issuance reviews and aggressive follow-up; root cause analysis (for poor and good quality); termination from peer review after repeat quality issues

Practice Monitoring of the Future
Long-term initiative for near real-time, ongoing monitoring of firm quality checks using robust technological platform

Enforcement
Aggressive investigation of all referrals of deficiencies; enhanced coordination with state boards of accountancy having ability to restrict license to practice; reinforced Code of Professional Conduct rules on due care

Knowledge Check:

What are the six core components of the plan to improve audits?

Sources

"CAQ Approach to Audit Quality Indicators." TheCAQ.org, April 2014: tinyurl.com/CAQAuditQualityIndicators (PDF)

"Enhancing Audit Quality: A 6-Point Plan to Improve Audits." AICPA.org, May 2015: tinyurl.com/AICPA6Point (PDF)

"Financial Firms Face Further Scrutiny of Their Cybersecurity Practices — Is Your Firm Ready?" ExternalIT.com, Sept. 15, 2015: tinyurl.com/pcyylub

"Performing Quality ERISA Employee Benefit Plan Audits: Firm Best Practices." AICPA.org: tinyurl.com/EBPAQCBestPractices (PDF)

"Security and Privacy." AICPA.org: aicpa.org/privacy

Singleton, Tommie. "The Top 5 Cybercrimes." AICPA.org, October 2013: tinyurl.com/p6wh4hw (PDF)

Chapter 4:
Conclusion

As always, individual CPAs and CPA firms are charged with upholding the changes detailed in this course. Where regulations don't dictate the proper course of action, the AICPA's conceptual frameworks offer guidelines for applying the ideals of the profession properly. Staying current on changes to ethical standards and best practices remains the best way to ensure ethical behavior.

Now that you know what's new in regulations and ethics for 2016, here are a few steps you can take to apply the concepts from this course to your own practice:

- Review the Knowledge Check on pages 4–5.
- Please complete the class evaluations that will be sent to you via email. We appreciate all feedback you provide, as it helps us make improvements to this course.
- Check the status of your CPA license (and firm license, if applicable) on the VBOA website.
- Make a note of the AICPA's Ethics hotline, (888) 777-7077, in case you have any pressing ethical questions.
- Make sure your CPE information is up to date in the VBOA's CPE tracker.
- Familiarize yourself with the standards contained in the AICPA's Code of Professional Conduct (tinyurl.com/pjck8g2).
- Review the trending topics discussed in this course and obtain further education on the ones relevant to your practice.

Visit vscpa.com/EthicsResources for the most up-to-date information on topics discussed in this course, as well as other resources to help you in your day-to-day decision-making. The VSCPA is proud to provide the highest-quality Ethics course for all Virginia CPAs. Thanks for learning with us!

Appendix I:
Resources, Glossary and Acronyms

As a licensed CPA, you are regulated by the state(s) in which you are licensed, among other bodies, depending on the nature of your work or your organization's work. The VBOA incorporates by reference (per § 54.1-4413.3) and sets forth that persons and firms using the CPA title in Virginia shall follow the standards and any interpretive guidance issued by the organizations listed in this section.

Code of Virginia:
Title 54.1 Professions and Occupations; Chapter 44 — Public Accountants: tinyurl.com/6f9ucox

AICPA Code of Professional Conduct:
In standard form: tinyurl.com/nh6bqkv
In topical (indexed) form: tinyurl.com/pjck8g2

Virginia Board of Accountancy (VBOA)
boa.virginia.gov
Email: boa@boa.virginia.gov
CPA Licensing Services & General Information: (804) 367-8505
CPA Examination Services: (804) 367-1111

VBOA Regulations
tinyurl.com/kvrlcqd

Virginia Society of CPAs
vscpa.com
(804) 270-5344
CPE Hotline: (800) 733-8272

VSCPA Ethics Resource Center
vscpa.com/EthicsResources
No matter when you choose to fulfill your Ethics requirement, you can always get the most up-to-date information about issues presented in the course at the VSCPA's Ethics Resource Center. While the information contained in this manual — including URLs, email addresses and phone numbers — is accurate as of the time the manual was printed, the VSCPA will be updating this page throughout the year.

American Institute of CPAs (AICPA)
aicpa.org
AICPA hotline: (888) 777-7077
The AICPA Ethics Hotline provides non-authoritative guidance to members on questions related to ethics, including independence. The Ethics Hotline is open from 9 a.m. – 5 p.m. EST on weekdays. A staff member can be reached via email at ethics@aicpa.org or via phone at (888) 777-7077, option 6, followed by option 1.

AICPA Technical Hotline
tinyurl.com/3drwcr5
(877) 242-7212

U.S. Comptroller General:
gao.gov/cghome/index.html

Financial Accounting Foundation (FAF)
accountingfoundation.org

Federal Accounting Standards Advisory Board (FASAB)
fasab.gov
(202) 512-7350

Financial Accounting Standards Board (FASB)
fasb.org
(203) 847-0700
Codification: asc.fasb.org/

U.S. Government Accountability Office (GAO)
gao.gov
(202) 512-3000

Government Accounting Standards Board (GASB)
gasb.org
(203) 847-0700

U.S. Internal Revenue Service (IRS)
irs.gov
(866) 255-0654

International Accounting Standards Board (IASB)
ifrs.org
+44 (0)20 7246 6410

Public Company Accounting Oversight Board (PCAOB)
pcaobus.org
(202) 207-9100
Independence and Ethics Rules and Standards (including AICPA Code of Professional Conduct references):
tinyurl.com/cxwr4l7

U.S. Securities and Exchange Commission (SEC)
sec.gov
(888) 732-6585

Appendix I:
Resources, Glossary and Acronyms

Glossary of Terms

Unless otherwise noted, the following definitions are from the Code of Virginia § 54.1-4400. Definitions.

Assurance means any form of expressed or implied opinion or conclusion about the conformity of a financial statement with any recognition, measurement, presentation or disclosure principles for financial statements.

Attest services means audit, review or other attest services for which standards have been established by the Public Company Accounting Oversight Board (PCAOB), by the Auditing Standards Board or the Accounting and Review Services Committee of the American Institute of CPAs (AICPA), or by any successor standard-setting authorities.

Compilation services means compiling financial statements in accordance with standards established by the AICPA or by any successor standard-setting authorities.

Financial statement means a presentation of historical or prospective information about one or more persons or entities.

Financial reporting framework (FRF) are the standards used to measure, recognize, present and disclose all material items within an entity's financial statements. Examples include U.S. Generally Accepted Accounting Principles (GAAP), International Financial Reporting Standards (IFRS) and special purpose frameworks.

Financial Reporting Framework for Small-and-Medium-sized Entities (FRF-SME) s a principles-based special purpose framework for preparing financial statements of privately held small- to medium-sized entities. It was developed under the guidance of the AICPA FRF for SMEs task force and is therefore non-authoritative.

Licensee means a person or firm holding a Virginia license or the license of another state. However, for purposes of this document, licensee only refers to a person holding a Virginia license or the license of another state.

Mobility means a practice privilege that generally permits a licensed CPA in good standing from a substantially equivalent state to practice outside of his or her place of business without obtaining another license. Source: www.cpamobility.org

Owner-managed entities are closely held companies run by the individuals who own a controlling ownership interest; a stark contrast to public companies, which by definition have an obvious separation between ownership and the management. *Source: AICPA's Financial Reporting Framework for Small- and Medium-sized Entities FAQ*

Peer review means a review of a firm's attest services and compilation services conducted in accordance with the monitoring program.

Practice of public accounting means the giving of an assurance other than (i) by the person or persons about whom the financial information is presented or (ii) by one or more owners, officers, employees or members of the governing body of the entity or entities about whom the financial information is presented.

Principal place of business is the primary location where a taxpayer's business is performed. The principal place of business is generally where the business's books and records are kept and is often where the head of the firm — or at least upper management — is located. This is discussed in the Virginia regulations: 18VAC5-22-50. Determining whether the principal place of business of a person using the CPA title, or of a firm, is in Virginia. Complying with subdivision A 1 of § 54.1-4409.1, subsection B of § 54.1-4411, or subsection B of § 54.1-4412.1 of the Code of Virginia requires the person or firm to use reasonable judgment in determining whether Virginia is the principal place of business in which the person provides services to the public using the CPA title or the firm provides attest services or compilation services. The determination shall be reasonable considering the facts and circumstances and can be based on quantitative or qualitative assessments. The determination shall be reconsidered for changes in facts and circumstances that are not temporary.

Providing services to the public using the CPA title means providing services that are subject to the guidance of the standard-setting authorities listed in the standards of conduct and practice in subdivisions 5 and 6 of § 54.1-4413.3.

§ 54.1-4413.3. Standards of conduct and practice. (5 and 6 only listed below.)

5. Follow the technical standards, and the related interpretive guidance, issued by committees and boards of the American Institute of Certified Public Accountants that are designated by the Council of the American Institute of Certified Public Accountants to promulgate technical standards, or that are issued by any successor standard-setting authorities.

6. Follow the standards, and the related interpretive guidance, as applicable under the circumstances, issued by the Comptroller General of the United States, the Federal Accounting Standards Advisory Board, the Financial Accounting Standards Board, the Governmental Accounting Standards Board, the Public Company Accounting Oversight Board, the U. S. Securities and Exchange Commission, comparable international standard-setting authorities, or any successor standard-setting authorities.

Providing services to an employer using the CPA title means providing to an entity services that require the substantial use of accounting, financial, tax or other skills that are relevant, as determined by the Board.

Small- and medium-sized entities (SME). There is no standard definition in the United States or under the AICPA. *Source: AICPA's Financial Reporting Framework for Small- and Medium-sized Entities FAQ*

Special purpose framework is a financial reporting framework for use in those situations where GAAP may not be required. Examples include tax and modified cash bases. The former term, OCBOA, was replaced with this term under SAS No. 122 section 800, effective Dec. 15, 2012. *Source: AICPA's Financial Reporting Framework for Small- and Medium-sized Entities FAQ*

Substantial equivalency means that the education, CPA exam and experience requirements contained in the statutes and administrative rules of another jurisdiction are comparable to, or exceed, the education, CPA exam and experience requirements contained in Chapter 44 of Title 54.1 of the Code of Virginia and the Board of Accountancy Regulations. (18VAC5-22)

Using the CPA title in Virginia means using "CPA," "Certified Public Accountant" or "public accountant" (i) in any form or manner of verbal communication to persons or entities located in Virginia or (ii) in any form or manner of written communication to persons or entities located in Virginia, including but not limited to the use in any abbreviation, acronym, phrase or title that appears in business cards, the CPA wall certificate, Internet postings, letterhead, reports, signs, tax returns or any other document or device.

Common Acronyms and Abbreviations

- **AICPA** — American Institute of CPAs
- **ASU** — Accounting Standards Update
- **CAQ** — Center for Audit Quality
- **CPA** — Certified Public Accountant
- **CPE** – Continuing Professional Education
- **EBPAQC** — AICPA Employee Benefit Plan Audit Quality Center
- **ET** — Ethics (topical index of the AICPA Professional Code of Conduct)
- **FAF** — Financial Accounting Foundation
- **FASB** — Financial Accounting Standards Board
- **FRF** — Financial reporting framework
- **GAO** — U.S. Government Accountability Office
- **IESBA** — International Ethics Standards Board for Accountants
- **IFAC** — International Federation of Accountants
- **IQAB** — International Qualification Appraisal Board
- **IQEX** – International Qualification Examination
- **IRC** — U.S. Internal Revenue Code
- **IRS** — U.S. Internal Revenue Service
- **GAAP** — Generally Accepted Accounting Principles
- **GAAS** — Generally Accepted Auditing Standards
- **GAGAS** — Generally Accepted Government Auditing Standards
- **GAPP** — Generally Accepted Privacy Principles
- **NASBA** — National Association of State Boards of Accountancy
- **PCAOB** — Public Company Accounting Oversight Board

Appendix I:
Resources, Glossary and Acronyms

- **PCC** — Private Company Council
- **PEEC** — AICPA Professional Ethics Executive Committee
- **PIOB** — Public Interest Oversight Board
- **PTIN** — Preparer Tax Identification Number
- **SHRM** — Society for Human Resource Management
- **SME** — Small- and medium-sized entities
- **SPF** — Special purpose framework (previously Other Comprehensive Basis of Accounting)
- **SSAE** — Statements on Standards for Attestation Engagements
- **SSARS** — Statements on Standards for Accounting and Review Services
- **SQCS** — Statement on Quality Control Standards
- **SSTS** — Statements on Standards for Tax Services
- **VAC** — Virginia Administrative Code ("Regulations")
- **VBOA** — Virginia Board of Accountancy ("the Board")
- **VSCPA** — Virginia Society of CPAs

Appendix II:
Additional Case Studies for 2016 Ethics

Major Donor

A CPA is listed in publications as a major donor to a charity for which his sole proprietorship is providing attest services.

- *Does this imply an appearance of impropriety?*
- *Could third-party users of the financial information reasonably expect true independence?*

Often, CPAs are called upon to provide services, often on a volunteer basis, to charities.

- *What are the risks in such arrangements?*
- *Is there a risk if a CPA provides "cut rate" services to a charity?*
- *As a volunteer, is the CPA obligated to be technically competent, perhaps in nonprofit areas, in order to volunteer?*

Dilemma at the Loading Dock

You are at the loading dock at year end to witness the client's shipping cut-off procedures. You witness the truck driver pull away from the dock and stop a few feet away with the rear door still open just before cut-off time. Shippers continue to load the truck after it stopss.

- *What are the potential ethics issues and responsibilities here?*

This real-life scenario has ethics implications for both members in practice and members in business. How you look at this scenario depends on your role and involvement in the situation. Shipping and revenue recognition policies are important to every stakeholder. For the auditor, this situation calls into question the strength of internal controls and application of company procedures, as well as financial statement accuracy and management decision-making. For the business, this situation could impact revenue recognized for the year, overall financial results and ultimately executive compensation. Interpretation of company policies is critical, and as we know, each of us has a different way of interpreting situations based on our own background, experience and culture.

The actions we take in a situation like this depend on our interpretations and involve trust, integrity and accountability, just for starters!

Rely on the Predecessor

The following summarizes portions of an actual case finalized in 2015 by the SEC.

Jimmy Johnson was engaged to perform a re-audit of the Dec. 31, 2012, year-end financial statements of six audit clients, as a result of the Public Company Accounting Oversight Board (PCAOB) revoking the registration of the predecessor auditor. In fact, Johnson had worked at the predecessor firm, then left and established his own practice, acquiring 18 new clients within two months of becoming registered with the PCAOB.

The SEC ruled that Johnson's re-audits of the Dec. 31, 2012, financial statements amounted to no audits at all, and the information he obtained from any review of the predecessor auditor's work papers was insufficient to afford a basis for expressing an opinion on the financial statements. Significant categories of work papers were either completely absent from the audit file or consisted of a schedule prepared by the client that detailed the particular account balance, but contained no other documentation from Johnson such as the procedures performed, evidence obtained, or conclusions reached. For example, virtually no work papers existed for two of the audits. The majority of work papers for one audit only contained a notation from Johnson indicating that he "traced to w/p in prior auditor file, reviewed procedures."

In addition to a six-figure fine, the SEC withdrew Johnson's PCAOB registration.

While the deficiencies in this case are clearly obvious, the situation did in fact occur.

- *As professionals, when a CPA follows the work of another CPA, whether in an audit setting or as a successor employee in a business or nonprofit entity, is a degree of professional skepticism needed when relying on the efforts of another CPA?*
- *How much skepticism is enough?*
- *Can there be too much skepticism?*

Appendix II:
Additional Case Studies for 2016 Ethics

Small Mistake

A four-partner CPA firm prepares financial statements for a closely-held medium size manufacturing company. The engagement is wrapping up and nothing remains but the delivery of the reports. As the bound audited financial statement is placed on the manager's desk for subsequent delivery to the client, it flips open and he immediately notices that the statement of financial position does not "foot." This is easy to see, since one of the asset balances ends in a one, all other amounts end in a zero, but the Total Assets ends in a zero. Realizing that this is probably a simple rounding error, the manager shakes her head, closes the binder and delivers the reports to the client. The mistake is probably one dollar or less. No harm, no foul?

This same issue could occur in a business, government or nonprofit, where the manager was the CFO who was preparing to deliver a report to her Board of Directors.

- *A dollar is truly immaterial. Is it worth the time to correct the problem?*
- *If the error is not corrected and subsequently discovered, what is the response from the audit manager or CFO?*
- *Does materiality play a factor in the situation? Should it?*
- *Would it make a difference if the error were not discovered by the CPA, but was only discovered later by the receiving party?*

Appendix III:
Section 7216 Sample Consent Forms

CONSENT TO DISCLOSURE OF TAX RETURN INFORMATION
Consent A

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose your tax return information to third parties for purposes other than the preparation and filing of your tax return without your consent. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form to engage our tax return preparation services. If we obtain your signature on this form by conditioning our tax return preparation services on your consent, your consent will not be valid. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year from the date of signature.

Please complete: (*To be completed by the taxpayer.)*

Purpose for disclosing information: _____
_____
_____

Name and address to whom the information is being disclosed:
_____
_____
_____
_____

Duration of consent: _____

I, _____, authorize (name of accounting firm/preparer) to disclose to _____ my tax return information for 20___.

Signature: _____ Date: _____

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by email to: complaints@tigta.treas.gov.

Appendix III:
Section 7216 Sample Consent Forms

CONSENT TO DISCLOSURE OF TAX RETURN INFORMATION
Consent B

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose your tax return information to third parties for purposes other than the preparation and filing of your tax return without your consent. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form to engage our tax return preparation services. If we obtain your signature on this form by conditioning our tax return preparation services on your consent, your consent will not be valid. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year from the date of signature.

You have indicated that you are interested in obtaining information on retirement plans such as an IRA, SEP, or Roth IRA, purchase or sale of investments, managed funds accounts, and/or other advice concerning your financial investments. To provide you with this information, (name of accounting firm/preparer) must disclose your tax return information, as indicated below to the (name of financial service firm) that provides this service

If you would like (name of accounting firm/preparer) to disclose your tax return information to (name of financial service firm) providing this service, please check the corresponding box for the service in which you are interested, provide the information requested below, and sign and date your consent to disclosure of your tax return information.

I, (INSERT NAME), authorize (name of accounting firm/preparer) to disclose to (name of financial service firm) that portion of my tax return information for (tax year (s)) that is necessary for (name of financial service firm) to contact me and provide information about the following topics:

___IRA, SEP, or Roth IRA retirement plans
___Purchase or sale of investments and managed funds accounts
___Other (please specify)
_____

If you approve use of your tax return information by (name of accounting firm/preparer) for a term of one year or (duration of consent date), please sign below.

Signature: _____

Print name: _____ Date: _____

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by email at complaints@tigta.treas.gov.

CONSENT TO DISCLOSURE OF TAX RETURN INFORMATION
Consent C

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot disclose your tax return information to third parties for purposes other than those related to the preparation and filing of your tax return without your consent. If you consent to the disclosure of your tax return information, Federal law may not protect your tax return information from further use or distribution.

You are not required to complete this form. Because our ability to disclose your tax return information to another tax return preparer affects the tax return preparation service(s) that we provide to you and its (their) cost, we may decline to provide you with tax preparation services or change the terms (including the cost) of the tax preparation services that we provide to you if you do not sign this form. If you agree to the disclosure of your tax return information, your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year from the date of signature.

This consent to disclose may result in your tax return information being disclosed to a tax return preparer located outside the United States, including your personally identifiable information such as your Social Security Number ("SSN"). Both the tax return preparer in the United States that will disclose your SSN and the tax return preparer located outside the United States that will receive your SSN maintain an adequate data protection safeguard (as required by the regulations under 26 U.S.C. Section 7216) to protect privacy and prevent unauthorized access of tax return information. If you consent to the disclosure of your tax return information, Federal agencies may not be able to enforce U.S. laws that protect the privacy of your tax return information against a tax return preparer located outside of the U.S. to which the information is disclosed.

If you (and your spouse) agree to allow ABC (U.S. based firm) to disclose your tax return information, including your SSN, to the foreign entity or entities listed below for purposes of providing assistance in the preparation of your (INSERT YEAR) individual tax return, please check the box below, provide the information requested, sign and date your consent to the disclosure of your tax return information.

I (We) authorize ABC to disclose to XYZ [foreign-based firm] my (our) tax return information including my (our) SSN(s) to allow XYZ to assist ABC in providing me (us) with tax return preparation services.

Name: _____ Name: _____
Signature: _____ Signature: _____
Date: _____ Date: _____

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484, or by e-mail at complaints@tigta.treas.gov.

Appendix III:
Section 7216 Sample Consent Forms

CONSENT TO USE OF TAX RETURN INFORMATION
Consent D

Federal law requires this consent form be provided to you. Unless authorized by law, we cannot use your tax return information for purposes other than the preparation and filing of your tax return without your consent.

You are not required to complete this form. If we obtain your signature on this form by conditioning our tax return preparation services on your consent, your consent will not be valid. Your consent is valid for the amount of time that you specify. If you do not specify the duration of your consent, your consent is valid for one year.

Taxpayer hereby consents to the use by (name of accounting firm/preparer) of any and all tax return information contained in the taxpayer's federal income tax returns (Forms 1040, 1040NR, 1040A, 1040EZ, etc. and supporting schedules) for the purpose of mailing, including electronic transmission, to the taxpayer information pertaining to:
____ Newsletters of accounting firm/preparer
____ Newsletters of affiliated financial planning firm to the accounting firm/preparer
____ Press releases and published articles of accounting firm/preparer
____ Upcoming seminars, webinars, and webcasts
____ Accounting firm/preparer promotion or hire announcements

The tax information may not be disclosed or used by (name of accounting firm/preparer) for any purpose other than that permitted by this consent document.

This consent will be valid for a period of three years beginning on January 1, 20__ and expire on December 31, 20__.

Alternative expiration date requested if not December 31, 20__: _____.

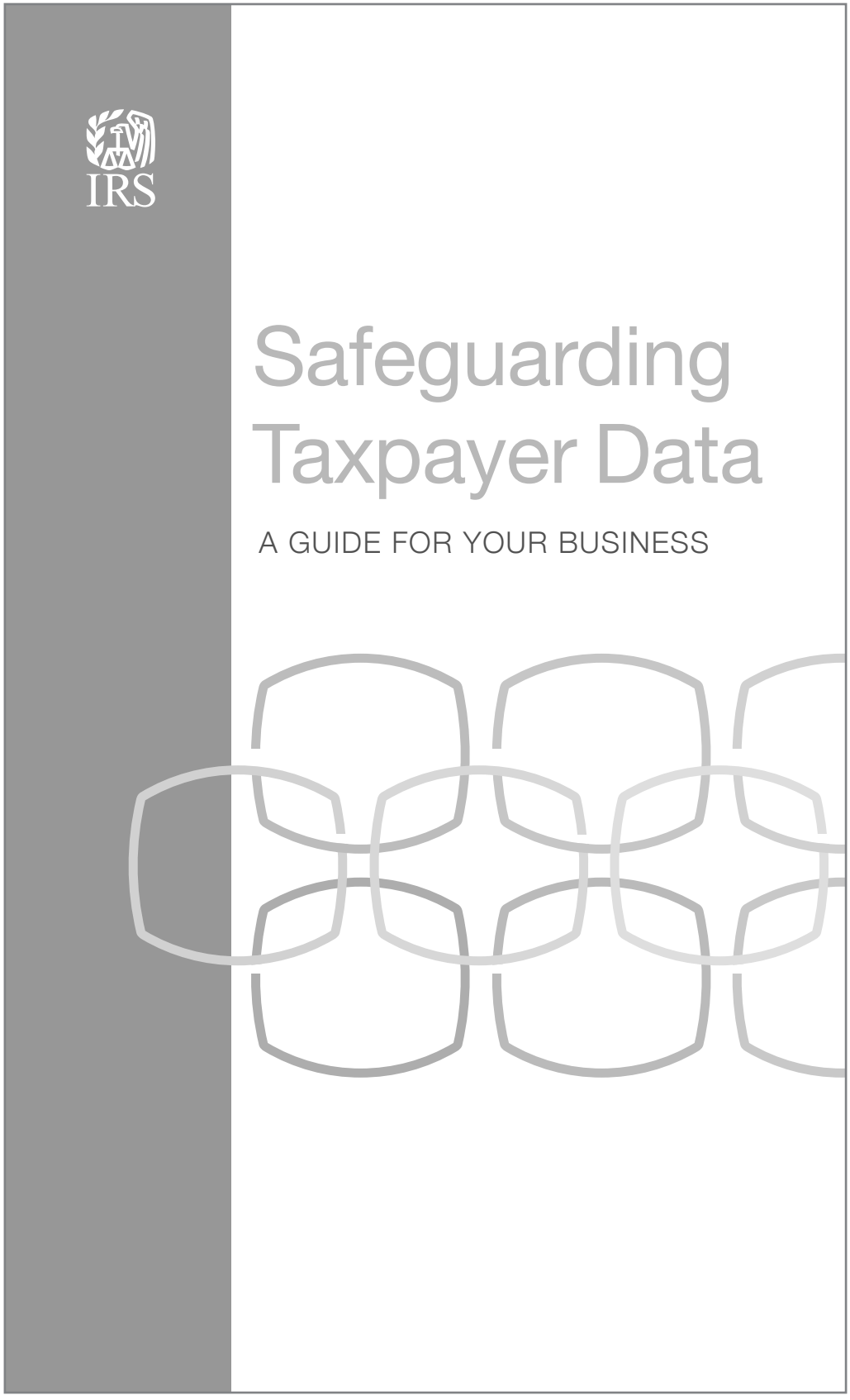
Signed this____ day of _____, 20____

Name (please print) _____

Signature _____

If you believe your tax return information has been disclosed or used improperly in a manner unauthorized by law or without your permission, you may contact the Treasury Inspector General for Tax Administration (TIGTA) by telephone at 1-800-366-4484 by email at complaints@tigta.treas.gov.

Appendix IV:
IRS Publication 4557



Appendix IV:
IRS Publication 4557

Contents

The Need to Safeguard Taxpayer Data

Today's identity thieves are a formidable enemy. They are an adaptive adversary, constantly learning and changing their tactics to circumvent the safeguards and filters put in place to stop them from committing their crimes. Some of the individuals committing identity theft refund fraud are members of high-tech global rings engaged in full-scale organized criminal enterprises for stealing identities and profiting from that information. As the criminals' efforts increase in sophistication, so do the number and scope of data breaches, which serves to further expand the network and warehousing of stolen and compromised identity information, and in turn increases the potential for that stolen identity information to ultimately reverberate through the tax system.

In 2015, the IRS called together major players in the tax industry—tax return preparers, software providers, state tax agencies, payroll providers and financial institutions—for a Security Summit to increase the cooperation in place to fight a common enemy—the identity thieves. Tax preparers are critical players in this partnership, and, because of the taxpayer information they store, increasingly a target for data theft.

Safeguarding taxpayer data is a top priority for the IRS. It is the legal responsibility of government, businesses, organizations, and individuals that receive, maintain, share, transmit or store taxpayers' personal information. Taxpayer data is defined as any information that is obtained or used in the preparation of a tax return (e.g., income statements, notes taken in a meeting, or recorded conversations). Putting safeguards in place to protect taxpayer information helps prevent fraud and identity theft and enhances customer confidence and trust.

This guide will help non-governmental businesses, organizations, and individuals that handle taxpayer data to understand and meet their responsibility to safeguard this information. IRS *e-file* and paper return preparers, Intermediate Service Providers, Software Developers, Electronic Return Originators, Reporting Agents, Transmitters, their affiliates, and service providers can use this guide to determine their data privacy and security needs and implement safeguards to meet them.

>

Appendix IV:
IRS Publication 4557

These safeguards will help you:

- Preserve the confidentiality and privacy of taxpayer data by restricting access and disclosure;
- Protect the integrity of taxpayer data by preventing improper or unauthorized modification or destruction; and
- Maintain the availability of taxpayer data by providing timely and reliable access and data recovery.

For a brief description of related laws and regulations, refer to the table in "Safeguarding Taxpayer Data, References to Applicable Laws and Regulations." For references to standards and best practices, refer to the table in "Safeguarding Taxpayer Data, References to Applicable Standards and Best Practices."

It is critical that we work in partnership to combat identity theft. Major software providers are required to report data thefts to the IRS. We urge individual tax preparers to notify their local IRS Stakeholder Liaison of any data theft to lessen the impact on clients and the tax system.

As the criminals' efforts increase in sophistication, so do the number and scope of data breaches, which serves to further expand the network and warehousing of stolen and compromised identity information, and in turn increases the potential for that stolen identity information to ultimately reverberate through the tax system.

Getting Started

If you handle taxpayer information, you may be subject to the Gramm-Leach Bliley Act (GLB Act) and the Federal Trade Commission (FTC) Financial Privacy and Safeguards Rules. Whether or not you are subject to the GLB Act and the FTC Rules, you could benefit from implementing the general processes and best practices outlined in FTC information privacy and safeguards guidelines.

Financial institutions as defined by FTC include professional tax preparers, data processors, their affiliates and service providers who are significantly engaged in providing financial products or services. They must take the following steps to protect taxpayer information. Other businesses, organizations and individuals handling taxpayer information should also follow these steps because they represent best practices for all.

- Take responsibility or assign an individual or individuals to be responsible for safeguards;
- Assess the risks to taxpayer information in your office, including your operations, physical environment, computer systems and employees, if applicable. Make a list of all the locations where you keep taxpayer information (computers, filing cabinets, bags, and boxes taxpayers may bring you);
- Write a plan of how you will safeguard taxpayer information. Put appropriate safeguards in place;
- Use only service providers who have policies in place to also maintain an adequate level of information protection defined by the Safeguards Rule; and
- Monitor, evaluate and adjust your security program as your business or circumstances change.

The FTC has fact sheets and guidelines on privacy and safeguards for businesses on their Web site at www.ftc.gov. In addition, you may seek outside professional help to assess your information security needs.

>

Appendix IV:
IRS Publication 4557

To safeguard taxpayer information, you must determine the appropriate security controls for your environment based on the size, complexity, nature and scope of your activities. Security controls are the management, operational, and technical safeguards you may use to protect the confidentiality, integrity and availability of your customers' information. Examples of security controls are:

1. Locking doors to restrict access to paper or electronic files;
2. Requiring passwords to restrict access to computer files;
3. Encrypting electronically stored taxpayer data;
4. Keeping a backup of electronic data for recovery purposes;
5. Shredding paper containing taxpayer information before throwing it in the trash;
6. Do not email unencrypted sensitive personal information.

Further, Authorized IRS e-file Providers that participate in the role as an Online Provider must follow the IRS six security, privacy, and business standards to better serve taxpayers and protect their individual income tax information collected, processed, and stored. See "Safeguarding IRS *e-file*" in Publications 1345 for more information.

All Authorized IRS e-file Providers who own or operate a Web site through which taxpayer information is collected, transmitted, processed, or stored must register their Uniform Resource Locator (URL). See instructions for submitting the URL information.

For additional examples of security controls, refer to the National Institute of Standards and Technology (NIST) SP 800-53 publication listed in "Safeguarding Taxpayer Data, References to Applicable Standards and Best Practices."

Putting Safeguards in Place

The following checklist includes many activities that can be included in an information security program. It can help you put in place security procedures and controls to protect taxpayer information.

It is important to consider all the safeguards that are applicable to your business.

>

Checklist 1

Administrative Activities

ONGOING	DONE	N/A	
☐	☐	☐	Complete a Risk Assessment. Identify the risks and potential impacts of unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that can be used to access taxpayer data. How vulnerable is your customer's data to theft, disclosure, unauthorized alterations or unrecoverable loss? What can you do to reduce the impact to your customers and your business in such an event? What can you do to reduce vulnerability?
☐	☐	☐	Write and follow an Information Security Plan that:
☐	☐	☐	• Addresses every item identified in the risk assessment.
☐	☐	☐	• Defines safeguards you want affiliates and service providers to follow
☐	☐	☐	• Requires a responsible person to review and approve the Information Security Plan.
☐	☐	☐	• Requires a responsible person to monitor, revise, and test the Information Security Plan on a periodic (recommended annual) basis to address any system or business changes or problems identified.
☐	☐	☐	Periodically (recommended annually) perform a Self-Assessment to:
☐	☐	☐	• Evaluate and test the security plan and other safeguards you have in place.
☐	☐	☐	• Document information safeguards deficiencies. Create and execute a plan to address them.
☐	☐	☐	Retain a copy of the Self-Assessment and ensure it is available for any potential reviews.
☐	☐	☐	If required by the FTC Privacy Rule, provide privacy notices and practices to your customers.
☐	☐	☐	Specify in contracts with service providers the safeguards they must follow and monitor how they handle taxpayer information.
☐	☐	☐	Ask service providers to give you a copy of their written security policy on safeguarding information.

Appendix IV:
IRS Publication 4557

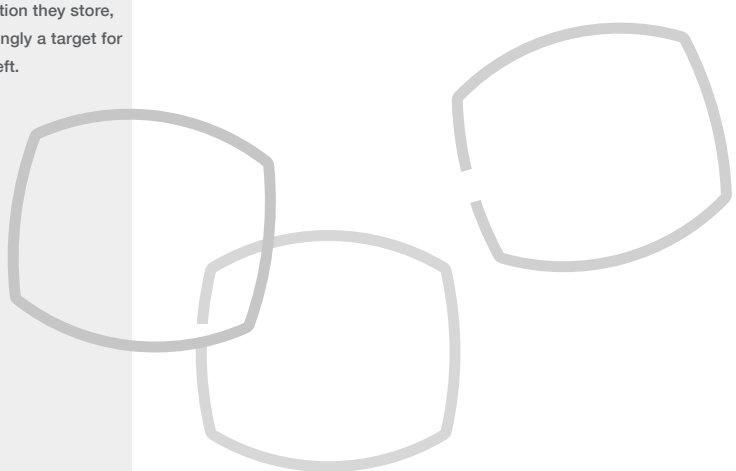
Checklist 2

Facilities Security

ONGOING	DONE	N/A	
☐	☐		Protect from unauthorized access and potential danger (e.g., theft, floods and tornados) all places where taxpayer information is located.
☐	☐		Write procedures that prevent unauthorized access and unauthorized processes.
☐	☐		Assure that taxpayer information, including data on hardware and media, is not left un-secured on desks or photocopiers, in mailboxes, vehicles, trash cans or rooms in the office or at home where unauthorized access can occur.
☐	☐		Authorize and control delivery and removal of all taxpayer information, including data on hardware and media.
☐	☐		Lock doors to file rooms and/or computer rooms.
☐	☐		Provide secure disposal of taxpayer information, such as shredders, burn boxes or temporary file areas until it can be securely disposed.

In 2015, the IRS called for a Security Summit to increase the cooperation in place to fight identity thieves.

Tax preparers are critical players in this effort, because of the taxpayer information they store, increasingly a target for data theft.



Checklist 3

Personnel Security

ONGOING	DONE	N/A	
☐	☐	☐	Create and distribute Rules of Behavior that describe responsibilities and expected behavior regarding computer information systems as well as paper records and usage of taxpayer data. Have all information system users complete, sign, and submit an acknowledgement that they have read, understood, and agree to comply with the rules of behavior. An example of rules of behavior can be found in Appendix A of NIST SP-800 18 *Guide for Developing Security Plans for Federal Information Systems*.
☐	☐	☐	Ensure personnel from third-party providers such as service bureaus, contractors, and other businesses providing information technology services meet the same security requirements as those applied to your personnel.
☐	☐	☐	Address Rules of Behavior for computer system management.
☐	☐	☐	When interviewing prospective personnel, explain the expected Rules of Behavior.
☐	☐	☐	When possible, perform a background and/or reference check on new employees who will have contact with taxpayer information. Conduct background screenings that are appropriate to the sensitivity of an assigned position.
☐	☐	☐	Screen personnel prior to granting access to any paper or electronic data. This will help ensure their suitability for a position requiring confidentiality and trust.
☐	☐	☐	Have personnel who will have access to taxpayer information sign nondisclosure agreements on the use of confidential taxpayer information.
☐	☐	☐	Develop and enforce formal compliance policies and processes, including possible disciplinary action, for all personnel who do not comply with the businesses' established information security policies and procedures.
☐	☐	☐	Terminate access to taxpayer information (e.g., login IDs and passwords) for those employees who are terminated or who no longer need access.
☐	☐	☐	For each employee who is terminated, conduct an exit interview and ensure the employee returns property that allows access to taxpayer information (e.g., laptops, media, keys, identification cards and building passes).
☐	☐	☐	Train staff on Rules of Behavior for access, non-disclosure and safeguards of taxpayer information. Provide refresher training periodically.

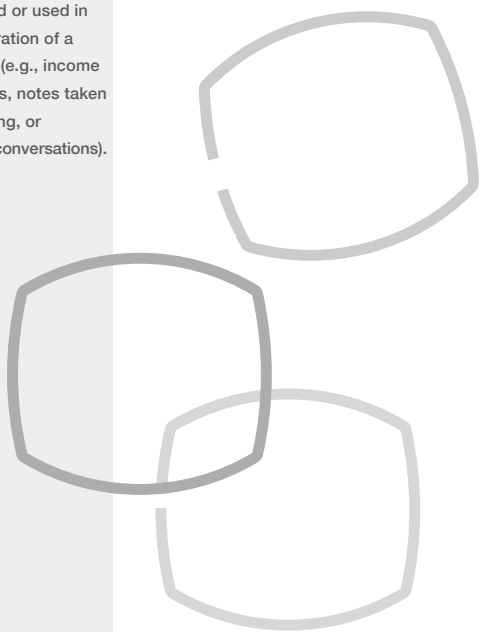
Appendix IV:
IRS Publication 4557

Checklist 4

Information Systems Security

ONGOING	DONE	N/A	
☐	☐		Information systems include both automated and manual systems made up of people, machines and/or methods for collecting, processing, transmitting, storing, archiving and distributing data. To help ensure the accuracy, validity, consistency and reliability of taxpayer data, you should manage taxpayer data information systems based on the guidelines below.
☐	☐		Grant access to taxpayer information systems only on a valid need-to-know basis that is determined by the individual's role within the business.
☐	☐		Put in place a written contingency plan to perform critical processing in the event that your business is disrupted. It should include a plan to protect both electronic and paper taxpayer information systems. Identify individuals who will recover and restore the system after disruption or failure.
☐	☐		Periodically test your contingency plan.
☐	☐	☐	Back up taxpayer data files regularly (e.g., daily or weekly) and store backup information at a secure location.
☐	☐	☐	Maintain hardware and software as needed and keep maintenance records.

Taxpayer data is defined as any information that is obtained or used in the preparation of a tax return (e.g., income statements, notes taken in a meeting, or recorded conversations).



Checklist 5

Computer Systems Security

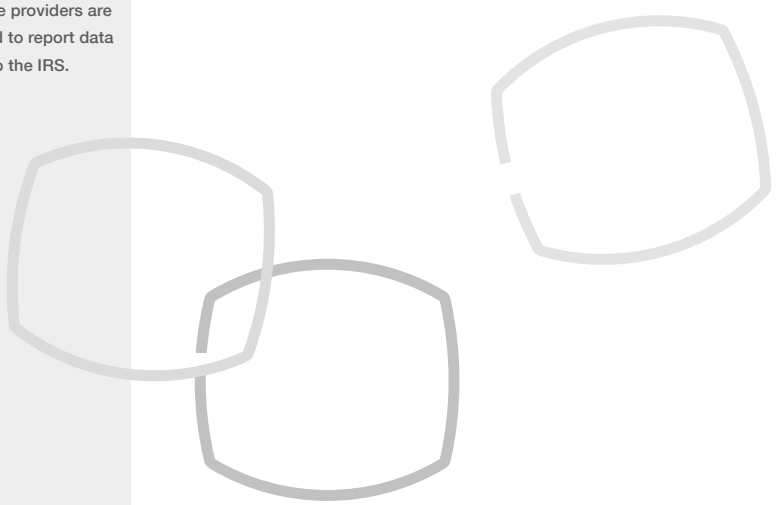
ONGOING	DONE	N/A	
☐	☐	☐	Identify and authenticate computer system users who require access to electronic taxpayer information systems before granting them access.
			You can manage user identities by:
☐	☐	☐	• Identifying authorized users of electronic taxpayer information systems and grant specific access rights/privileges.
☐	☐	☐	• Assigning each user a unique identifier.
☐	☐	☐	• Verifying the identity of each user.
☐	☐	☐	• Disabling user identifiers after an organization-defined time period of inactivity.
☐	☐	☐	• Archiving user identities.
☐	☐	☐	Implement password management procedures that require strong passwords.
☐	☐	☐	Require periodic password changes.
☐	☐	☐	Disable and remove inactive user accounts.
☐	☐	☐	Protect electronic taxpayer information systems connected to the Internet with a barrier device (e.g., firewall, router or gateway). Any failure of these devices should not result in an unauthorized release of taxpayer data.
☐	☐	☐	When storing taxpayer information electronically, consider following best practices and store it on separate secure computers or media that are not connected to a network and that are password protected and encrypted.
☐	☐	☐	Encrypt taxpayer information when attached to email.
☐	☐	☐	Encrypt taxpayer information when transmitting across networks.
☐	☐	☐	Regularly update firewall, intrusion detection, anti-spyware, anti-adware, anti-virus software and security patches.
☐	☐	☐	Monitor computer systems for unauthorized access by reviewing system logs.
☐	☐	☐	Lock out computer system users after three consecutive invalid access attempts.
☐	☐	☐	Remove all taxpayer information once the retention period expires by using software designed to securely remove data from computers and media prior to disposing of hardware or media. The FTC Disposal Rule has information on how to dispose of sensitive data.
☐	☐	☐	As recommended by the FTC, reduce risks to computer systems by performing vulnerability scans and penetration tests periodically. You can learn more about this at the FTC Web site in their article “FTC Facts for Business – Security Check: Reducing Risks to Your Computer Systems.”

Appendix IV:
IRS Publication 4557

Checklist 6

ONGOING	DONE	N/A	Media Security
☐	☐	☐	Store computer disks, removable media, tapes, compact disks, flash drives, audio and video recordings of conversations and meetings with taxpayers, and paper documents in a secure location, cabinet, or container.
☐	☐	☐	Secure media storage areas, including rooms, cabinets, and computers by locks or key access. Where appropriate, employ an automated mechanism to ensure only authorized access.
☐	☐	☐	Restrict authorized access to media storage.
☐	☐	☐	Limit removal of taxpayer information to authorized persons and perform information access audits regularly.
☐	☐	☐	Securely remove all taxpayer information when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media that contain taxpayer information. The FTC Disposal Rule has information on how to dispose of sensitive data.
☐	☐	☐	Shred or burn paper documents before discarding them.

It is critical that we work in partnership to combat identity theft. Major software providers are required to report data thefts to the IRS.



Checklist 7

Certifying Information Systems For Use

ONGOING	DONE	N/A	
☐	☐	☐	Determine if risks are acceptable to certify systems for use.
☐	☐		Sign an authority to operate.
			If you use a certified independent certification company, consider the following:
☐	☐		• On a periodic (recommended annual) basis, have an independent individual or business with relevant security expertise, evaluate the security plans, controls, and any other safeguards implemented in your business against best practices.
☐	☐		• Have a report generated from the audit that certifies that your business follows best practices.
☐	☐		• Ensure the report highlights any deficiencies and provides recommendations for their correction.
☐	☐		• Develop a plan for your business to correct any deficiencies found and to ensure that the plan is successfully executed.
☐	☐		• Retain a copy of the audit report to ensure it is available for any potential reviews.
☐	☐		• Be prepared to show how you mitigate risks.

Appendix IV:
IRS Publication 4557

Reporting Incidents

Safeguarding personally identifiable taxpayer information is of critical importance to retaining the confidence and trust of taxpayers. Appropriately handling information security incidents is also very important to retaining the confidence and trust of taxpayers.

An information security incident is an adverse event or threat of an event that can result in an unauthorized disclosure, misuse, modification or destruction of taxpayer information. If you believe an information security incident has occurred that affects the confidentiality, integrity, or availability of taxpayer data or the ability for the taxpayer to prepare or file a return, you may need to report the incident. The following table includes examples of types of incidents.

INCIDENT TYPE	DESCRIPTION
Theft	Unauthorized removal of computers, data/records on computer media or paper files.
Loss/Accident	Accidental misplacement or loss of computers, data/records on computer media or paper files.
Unauthorized Access	A person or computer gains logical or physical access without permission to a network, system, application, data, or other resource.
Unauthorized Disclosure/ Usage	A person violates disclosure or use policies such asIRC sections 6713 & 7216. See “Laws and Regulations” for information on IRC sections 6713 & 7216.
Computer System/ Network Attack	A virus, worm, Trojan horse, or other code-based malicious entity infects a host and causes a problem such as disclosure of sensitive data or denial of services.

Recommended actions for incident reporting are as follows:

- Individuals (e.g., employees and contractors) who detect a situation that may be an information security incident should immediately inform the individual designated by the business to be responsible for handling customer information security.
- The individual responsible for handling customer information security should gather information about the suspected incident.
- If you believe the incident compromises a person’s identity or their personal or financial information, we recommend you refer to the FTC document, Information Compromise and the Risk of Identity Theft: Guidance for Your Business. Among other things, this reference will help you determine when to notify local law enforcement, the Federal Bureau of Investigation, the U.S. Secret Service, the U.S. Postal Inspection Service, affected businesses, and customers. See the “Safeguarding Taxpayer Data, References to Applicable Standards and Best Practices” table for the Internet link to this FTC document.

Laws and Regulations

Many federal, state, city, and local government laws and regulations are in place to safeguard taxpayer data. The following table includes a brief description of some of them and provides references to more detailed information.

TYPE	SUMMARY OF APPLICABLE LAWS AND REGULATIONS
Federal/Privacy and Security	The *Gramm-Leach-Bliley Financial Modernization Act of 1999* – This statute (otherwise known as the Gramm-Leach-Bliley Act) (GLB Act), among other things, directed FTC to establish the Financial Privacy Rule and the Safeguards Rule.
Federal/Security	*FTC Standards for Safeguarding Customer Information Rule (16 CFR Part 314)* – This Rule (otherwise known as the Safeguards Rule) requires financial institutions, as defined, which includes professional tax preparers, data processors, affiliates, and service providers to ensure the security and confidentiality of customer records and information. It protects against any anticipated threats or hazards to the security or integrity of such records. In addition, it protects against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. This Rule requires that financial institutions develop, implement and maintain an Information Security Program. The plan should be written in one or more accessible parts and contain administrative, technical, and physical safeguards that are appropriate to the business' size and complexity, nature and scope of activities, and sensitivity of customer information handled.
	Sarbanes-Oxley Act of 2002 (17 CFR Parts 232, 240 and 249) – Section 404 requirements apply to all Securities and Exchange Commission (SEC) reporting companies with a market capitalization in excess of $75 million. It requires companies to establish an infrastructure to protect and preserve records and data from destruction, loss, unauthorized alteration or other misuse. This infrastructure must ensure there is no room for unauthorized alteration of records vital to maintaining the integrity of the business processes.

>

Appendix IV:
IRS Publication 4557

TYPE	SUMMARY OF APPLICABLE LAWS AND REGULATIONS
Federal/Privacy	*FTC Privacy of Consumer Financial Information Rule (16 CFR Part 313)* – This Rule (otherwise known as the Financial Privacy Rule) aims to protect the privacy of the consumer by requiring financial institutions, as defined, which includes professional tax preparers, data processors, affiliates, and service providers to give their customers privacy notices that explain the financial institution's information collection and sharing practices. In turn, customers have the right to limit some sharing of their information. Also, financial institutions and other companies that receive personal financial information from a financial institution may be limited in their ability to use that information. The FTC Privacy Rule implements sections 501 and 502(b)(2) of the GLB Act requirements.
	Title 26: Internal Revenue Code (IRC) § 301.7216.1 – This provision imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return.
	Title 26: Internal Revenue Code (IRC) § 6713 – This provision imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.
	Internal Revenue Procedure 2007-40 – This procedure requires Authorized IRS e-file Providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that violations of the GLB Act and the implementing rules and regulations promulgated by the FTC, as well as violations of the non-disclosure rules contained in IRC sections 6713 and 7216 or the regulations promulgated there under are considered violations of Revenue Procedure 2007-40, and are subject to penalties or sanctions specified in the Revenue Procedure.
State/Privacy and Security	*State Laws* – Many state laws govern or relate to the privacy and security of financial data, which includes taxpayer data. They extend rights and remedies to consumers by requiring individuals and businesses that offer financial services to safeguard nonpublic personal information. For more information on state laws that your business must follow, consult state laws and regulations.

Standards and Best Practices

Federal and state governments as well as private industry provide many information security standards and best practice guidelines to safeguard consumer information such as personal tax data. The National Institute of Standards and Technology (NIST) provides security guidelines and practices for federal agencies that nongovernmental organizations may also use. Below is a list of references on a variety of information safeguard topics that can help you understand and comply with laws, regulations and best practices that may apply to your business.

TYPE	REFERENCES TO APPLICABLE STANDARDS AND BEST PRACTICES
Federal/Privacy	"Getting Noticed: Writing Effective Financial Privacy Notices"
	"Information Compromise and the Risk of Identity Theft: Guidance for Your Business"
Federal/Security	"FTC Facts for Business: Financial Institutions and Customer Information: Complying with the Safeguards Rule"
	FTC Disposal Rule (2005) – "FTC Business Alert: Disposing of Consumer Report Information? Rule Tells How"
	"Security Check: Reducing Risks to Your Computer Systems"
	NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems: Provides guidance on developing an Information Security Plan and includes a sample plan in Appendix A.
	NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations
	NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide
	NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments
Private Industry/ Security	Industry Standards and Best Practices – Many private industry companies provide best practice advice on protecting information systems and safeguarding customer data. You can get more information on industry standards and best practice by researching the Internet and other resources.

Appendix IV:
IRS Publication 4557

Glossary

Adware
Computer advertising software that may or may not monitor computer use to target ads.

Authorized IRS e-file Provider
A business authorized by the IRS to participate in IRS e-file as an Electronic Return Originator, an Intermediate Service Provider, a Reporting Agent, a Software Developer, an Online Provider, or a Transmitter.

Confidentiality
Restrictions placed on information access and disclosure, including means for protecting personal privacy and proprietary information.

Denial of Service
An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources.

Electronic Return Originator (ERO)
Authorized IRS e-file Provider that originates the electronic submission of returns to the IRS.

Encrypt
To convert plain text to unintelligible text using a cryptographic algorithm.

Identity Theft
Misuse of someone else's personal information to obtain new accounts or loans or commit other crimes.

Information Resources
Information and related resources, such as staffing, funding and information technology.

Information Security
The process that ensures the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

Information System
A set of information resources designated for the organization of data for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Information Technology
Equipment, system or subsystem of equipment that is used in the handling of data. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources.

Integrity
The authenticity or unimpaired condition of information; including reliability for non-repudiation of origin.

Intermediate Service
Provider receives tax information from an ERO (or from a taxpayer who files electronically using a personal computer, modem, and commercial tax preparation software), processes the tax return information, and either forwards the information to a Transmitter or sends the information back to the ERO (or taxpayer for Online Filing).

Intrusion Detection
The act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource.

IRS *e-file*
The brand name of the electronic filing method established by the IRS.

Management Safeguards
The security safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

Non-repudiation
The process in which there is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity for future validation purposes.

Online Provider
An Online Provider allows taxpayers to self-prepare returns by entering return data directly into commercially available software, software downloaded from an Internet site and prepared off-line, or through an online Internet site.

Operational Safeguards
Security for an information system that is primarily implemented and executed by people rather than by a system.

Reporting Agent
originates the electronic submission of certain returns for its clients and/or transmits the returns to the IRS. A Reporting Agent must be an accounting service, franchiser, bank, or other entity that complies with Rev. Proc. 2012-32, 2012-34 I.R.B. 267, and is authorized to perform one or more of the acts listed in Rev. Proc. 2012-32 on behalf of a taxpayer. Reporting Agents must submit Form 8655, Reporting Agent Authorization, to the IRS prior to or at the same time that they submit an IRS e-file Application.

Risk
The likelihood that the unwanted impact of an incident will be realized.

Risk Assessment
The process of identifying risks and determining the probability of occurrence, the resulting impact and additional security controls that would mitigate this impact.

Risk Management
The process of managing risks through risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process includes consideration of effectiveness, efficiency and constraints due to laws, directives, policies, or regulations.

Safeguard
Protective measures prescribed to meet the security requirements specified for an information system. Safeguards may include security features, management constraints, personnel security and security of physical structures, areas, and devices.

Security Controls
Safeguards designed to protect the confidentiality, integrity and availability of a system and its information.

Security Plan
Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Appendix IV:
IRS Publication 4557

Security Requirements
Requirements that are derived from laws, policies, instructions, regulations or business (mission) needs to ensure the confidentiality, integrity and availability of the information being processed, stored or transmitted.

Service Provider
Any individual or business that maintains, processes, or is given access to customer information through the provisions of a service agreement with another individual or business.

Software Developer
develops software for the purposes of formatting electronic return information according to IRS *e-file* specifications and/or transmitting electronic return information directly to the IRS.

Spyware
Software installed into an information system to gather information on individuals or organizations without their knowledge.

Tax Preparer
Any person who is engaged in the business of preparing or assisting in preparing tax returns.

Technical Safeguards
Controls for a system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system.

Threat
Any circumstance or event with the potential to adversely impact operations, assets or individuals through an information system via unauthorized access, destruction, disclosure, modification of information and/or denial of service.

Transmitter
transmits electronic tax return information directly to the IRS. EROs and Reporting Agents may apply to be Transmitters and transmit return data themselves, or they may contract with accepted Third-Party Transmitters that will transmit the data for them. A Transmitter must have software and computers that allow it to interface with the IRS.

Trojan Horse
A computer program used to attack a computer system by secretly allowing, among other things, unauthorized access or alteration of data or software.

User
Individual or system process authorized to access an information system.

Virus
A computer program used to compromise a computer system by performing functions that may be destructive. A virus may alter other programs to include a copy of itself and execute when the host program or other executable component is executed.

Vulnerability
Weakness in a system through procedures, internal controls or implementation that could be exploited or triggered by a threat source.

Worm
A computer program used to compromise a computer system by impacting performance. A worm can travel from computer to computer across network connections replicating itself.

IRS

NOTE: The Internal Revenue Service prepared this guide as an outreach educational effort for all tax preparers, transmitters, and software developers. If you have any comments or suggestions for future updates, please send an e-mail to:

Safeguard.data.tp@irs.gov

Publication 4557 (Rev. 10-2015) Catalog Number 48905Y Department of the Treasury **Internal Revenue Service** www.irs.gov

Notes

Notes

Virginia Society of CPAs
4309 Cox Road
Glen Allen, VA 23060
p (800) 733-8272 • f (804) 273-1741
www.vscpa.com

Virginia Society of Certified Public Accountants