Controls over Federal Compliance
August 2025

IL T&TA
INDEPENDENT LIVING
TRAINING AND TECHNICAL ASSISTANCE CENTER

Presenters:
John Heveron, Jr. CPA
Paula L. McElwee

Before We Begin - Accessibility

- ASL & Spanish Interpreters are available and labeled
- Access Closed Captioning by clicking the CC button located at the bottom of your Zoom window
- Use Zoom's Raise Hand or Chat features to ask questions
- Remember to state your name before speaking
- Message our IL T&TA team using the Chat feature if you have difficulties with today's call
- Please complete the survey at the end of today's training

What You Will Learn

- **The requirements for controls over federal funds**
- **How to document your controls and be sure they are followed**
- **Understand how internal controls ensure adherence to federal requirements**
- **How to protect yourself from cyber threats**

What You Will Learn

Paula McElwee

Director of Technical Assistance

IL T&TA Center

John Heveron, Jr. CPA

Consultant, IL T&TA Center

Principal, Heveron and Company CPAs

Controls over federal compliance

The objectives of controls over compliance include—

- Ensure financial statements and federal reports are properly prepared and accurate
- Ensure key fiscal processes have adequate checks and balances
- Keep track of and protect assets
- Show you're following federal rules and grant terms
- Protect personal and confidential information

Compliance Requirements that may Directly Impact Your Programs

Potential areas of required compliance include:

- Specific funding sources including grant numbers.
- What activities are allowed or unallowed.
- What costs are allowable.
- Cash management (timing of and documenting draws).
- Eligibility of persons served.
- Matching requirements.
- Period of performance.
- Required reporting.

Compliance Requirements that may Directly Impact Your Programs (cont'd)

- Not all the above areas apply to all funding sources, although most will generally apply such as activities allowed or unallowed, allowable costs/cost principles, cash management, eligibility, and period of performance.
- When any of these areas apply and they are **direct** and **material**, you need to have (and document that you have) controls over those areas.
  - Direct – clearly traced to a specific transaction, account, or activity
  - Material – significant enough to influence decisions, outcomes, or risk exposure
- Do you always know which grant you are applying costs to and are you consistent? You should be.

Comprehensive Check of Overarching Internal Control Requirements

1. Does the grantee have adequate staffing, systems, and processes to provide reasonable assurance that ACL awards are utilized in line with applicable acts, statutes, regulations, and award terms and conditions?
2. Does the CIL board have clearly defined internal control responsibilities and are they being consistently implemented?
3. Are duties and responsibilities adequately segregated to ensure that key fiscal processes have adequate checks and balances?
4. Are fiscal processes and procedures codified into grantee policy and is the policy current?
5. Does the grantee have an internal review or evaluation process to assess compliance with its own policies and processes?
6. Does the grantee have policies regarding budget modifications and are they being consistently implemented?

Source: ACL IL Grant Programs Fiscal Review Checklist

Examples of Internal Controls

Specific controls over allowable activities and allowable costs/cost principles must include items such as:

- Review of contracts by a knowledgeable person to identify allowable activities, the overall budget, whether certain costs or activities require preapproval.

Specific controls over cash management might include:

- Review of the contract to determine the drawdown method, and assess the process for documenting drawdowns, and
- Develop a reporting system to identify any lapses between drawdowns and disbursement.

Examples of Internal Controls cont'd

- Specific period of performance controls could include:
  - Review of contracts to identify when services may be performed, and any unique requirements about pre-award spending, extensions, and repayment of unused amounts.
  - A review of your three-year program plan and assurance that you are spending federal funds in keeping with the purpose of independent living funds.

Guidance on Internal Controls

Part 6 of the 2024 Compliance Supplement provides guidance on internal controls. It emphasizes that internal control should be in compliance with guidance from COSO and the Green Book. COSO is the Committee on Sponsoring Organizations- accounting and financial leadership organizations, and the Green Book covers internal controls for governmental entities. These are both similar, identifying 5 key areas of control and 17 principles.

5 Key Areas of Internal Control

1. The Control Environment - your commitment to integrity and ethical values, your oversight and commitment to competence and accountability (ongoing training is big),
2. Risk Assessment - identifying and analyzing risks, and assessing fraud risks,
3. Control Activities - the policies and procedures you adopt for accounting and documentation, and your controls over technology,

5 Key Areas of Internal Control cont'd.

4. Information and Communication - your internal communications and training and external communications about your policies, procedures, and values, and,
5. Monitoring Activities - your ongoing assessment of whether controls are appropriate for your current programs and whether they are being followed.

Control Activities

- When it comes to internal controls, whether agency wide or specifically related to a grant or contract: **If you didn't document it, you didn't do it.**
- This is true for establishing a proper control environment, performing risk assessment, establishing control activities, communicating your procedures, policies and control activities, and monitoring.
- Independent auditors performing compliance audits are required to look at your controls over compliance and ACL and other funder auditors will as well.

Control Activities cont'd.

- You are probably performing certain monitoring activities such as budget development and comparison of budgeted to actual results, insurance/risk assessment, review of receivables/payables aging, monitoring liquidity, and discussing cash controls.
- There are several additional things you can do to monitor your controls. Review and discuss these (possibly in an executive or finance committee) select some, document the selection and the discussion as well as the execution of the procedures you select.
- You can monitor different areas such as the areas below on a rotating basis possibly covering each area every 3rd year.

Possible Monitoring Procedures

- Review the hiring process, personnel files, or payroll oversight.
- Review fundraising communications for accuracy and integrity.
- Verify that bank accounts are reconciled in a timely way.
- Review the purchasing process.
- Assess the physical security of confidential information.
- Review charge card documentation and expense reimbursements.
- Look at the process for training staff.
- Ask staff if their training and mentoring is sufficient.

A remote or partially remote workforce may call for some changes in your monitoring procedures.

CILs and SILCs are Responsible for Security

- “Individually identifiable data” is data that identifies the person that the data is about.
- “Individually Identifiable Health Information” is personal health information protected by HIPAA and other regulations.
- CILs and SILCs must take actions to limit cyber security risks.
- CILs and SILCs must take all reasonable measures to protect the confidentiality of this information.

CILs and SILCs are Responsible for Security cont'd

- This means physical and technical security of employee and consumer information.
- It means limiting access and testing security, possibly with intrusion detection systems.
- A disaster recovery plan can increase security.

Cybersecurity Risks

- Businesses and nonprofits get hacked every day.
- The group that video monitors presidential motorcades got randomly hacked by a couple in eastern Europe.
- The most recent Association of Certified Fraud Examiners *Report to the Nations* confirms extensive cybersecurity breaches including those at nonprofit organizations. https://legacy.acfe.com/report-to-the-nations/2024/
- Let's look at some resources to avoid ending up in the same boat.

Cybersecurity Risks cont'd

- What do cyber criminals want? money from your accounts, ransom (money from you), credit card numbers, Social Security numbers (that they can sell for money).
- How badly do they want these things? They are willing to spend their entire lives trying to trick you and steal from you – all day, every day. And, they are well paid.
- How can you reduce cybersecurity hacks by 90%?

Security over financial accounts

Falsified checks and bank account hijacks can be reduced with technology countermeasures, such as:

- Secure checks.
- Positive pay (provide your bank with information about checks you have issued for matching).
- Reverse positive pay (review incoming checks before they are processed).
- Using a secure font and inserting asterisks above the payee name to prohibit adding another name.

Security over financial accounts cont'd

- Do not provide a bank with confidential information unless you initiated the call.
- Do not respond to a bank e-mail request to click on a hyperlink.
- Look for the https://protocol on banking and other websites.

IT Security

- Servers and workstations should only use operating systems that are currently supported—Windows 10 support ends October 14, 2025.
- Operating system updates and patches should be installed promptly.
- Backups should be stored off-site or in the cloud frequently enough to avoid a significant loss of data.

IT Security cont'd

- IT and IT security training should be provided at various times throughout the year. Include cybersecurity and social engineering awareness (recognizing and avoiding risky email attachments, questionable downloads, and fake voicemail).
- Workstations should be set for automatic log off after a certain time.

IT Security cont'd 2

- Backups should be verified periodically to make sure they are working.
- All computers should have surge protectors and servers should have properly configured UPS/battery backups.
- Access to programs should be limited based on need for access.
- Access should be removed for anyone who leaves or is terminated.

IT Security cont'd 3

- Hard drives should be defragmented periodically.
- License and warranty information should be maintained in a secure central location.
- Strongly consider an outside organization for continuous remote monitoring and for updates and problems.

Cybersecurity Defense

- Train your staff in cybersecurity awareness.
- Periodically remind staff of the threats, risks and potential impact of cyber attacks.
- Make cybersecurity part of staff meetings.
- Here you can find a video and some guidance on reducing cybersecurity attacks.
- https://www.youtube.com/playlist?list=PLmvQaMcWIqbtQp81nL_g63NlOqzRRkTds 45 second closed-captioned tips for security.
- Short tips of the day. https://inspiredelearning.com/resource/security-awareness-tip-day/

Cybersecurity Defense cont'd

- The NIST (National Institute of Standards) Cybersecurity Framework provides a foundation for building or improving a cybersecurity program.
- The framework includes five functions: **Identify, Detect, Respond, Protect, and Recover**.
- **Identify** means that we will identify all people, devices and programs that are able to access our systems.
- **Detect** involves activities that enable us to detect cybersecurity events in a timely way.

Cybersecurity Defense cont'd 2

- The three objectives of information security include **confidentiality, integrity** and **availability**.
- **Confidentiality** protects sensitive or classified data from unauthorized access or disclosure.
- **Integrity** involves maintaining data accuracy, completeness, and consistency throughout its life cycle.
- **Availability** ensures that authorized users have timely and uninterrupted access to the resources and services they need.

Cybersecurity Defense cont'd 3

- We will promptly **respond** to cybersecurity incidents, including conducting analysis.
- **Protect** - every server, computer, and attached mobile device should have anti-virus and anti-malware software installed and running in real-time. This includes in-house devices as well as any remote or others that have access
- **Recover** by working to restore normal access including eliminating any unauthorized access, and promptly restoring from backups.

Cybersecurity Defense cont’d 4

- Wireless access points should be secured with passwords and clients/guests will only have access to separate wireless access points.
- Employees should never click on the "ok" button on popup windows. These could download malware. To close popups, click on the X in the upper right corner or press "Ctrl-W."
- Disable the "AutoRun/autoplay" feature that automatically executes content on a CD/DVD/USB drive.
- When available, activate two-factor authentication.

Cybersecurity Defense cont'd 5

- When employees leave, voluntarily or otherwise, company-owned devices must be returned, and account access must be shut down at the time of departure.
- Hackers like to put malicious code on USB drives and leave them in areas where employees might find them. Never plug in outside USB drives.
- Disposal of computers, copiers, and other physical assets that may contain confidential information should be properly disposed of through a certified disposal company. Obtain a certificate of destruction for these devices. Media such as CDs and USBs should be physically destroyed.

Questions

Resources

- Consider reaching out to an IT security firm. Even if you choose not to hire them you would still get some benefit from their recommendations.
- The NIST (National Institute of Standards) Cybersecurity Framework has has guidance and resources for cyber security https://www.nist.gov/cyberframework
- https://www.techsoup.org/ also provides useful IT and security resources
- The nonprofit risk management center has risk resources at https://nonprofitrisk.org/
- The COSO internal control framework can be found at https://www.coso.org/internal-control
- The Green Book internal control format can be found at https://www.gao.gov/products/gao-14-704g
- ACL IL Grant Programs Fiscal Review Checklist https://acl.gov/sites/default/files/programs/2024-12/ACL%20IL%20Grant%20Programs%20Fiscal%20Review%20Checklist%20-%20Published%2012.10.2024.docx

Evaluation

Thank you for participating in today's training.

Your feedback is important. Please use the link in the chat to share your feedback.

Contact Information

Independent Living Training & Technical Assistance Center

Rural Institute for Inclusive Communities at the University of Montana

📞 (406) 243-5300

✉️ ilttacenter@mso.umt.edu

🌐 www.ILTTACenter.org

👉 Stay Connected Email Sign Up | Facebook | LinkedIn | Instagram

The Independent Living Training & Technical Assistance Center is on assignment with the U.S. Department of Health and Human Services, Administration for Community Living.

Independent Living Training and Technical Assistance Center

The Independent Living Training and Technical Assistance Center (IL T&TA Center) is available to you through a **contract with the US Department of Health and Human Services**.

The IL T&TA Center provides **expert training and technical assistance** to Centers for Independent Living (CILs), State Independent Living Councils (SILCs), and Designated State Entities (DSEs).

The Center is operated by the University of Montana's **Rural Institute for Inclusive Communities.**

UNIVERSITY OF MONTANA

IL T&TA
INDEPENDENT LIVING
TRAINING AND TECHNICAL ASSISTANCE CENTER