ACUA

WEBINARS

ACUA

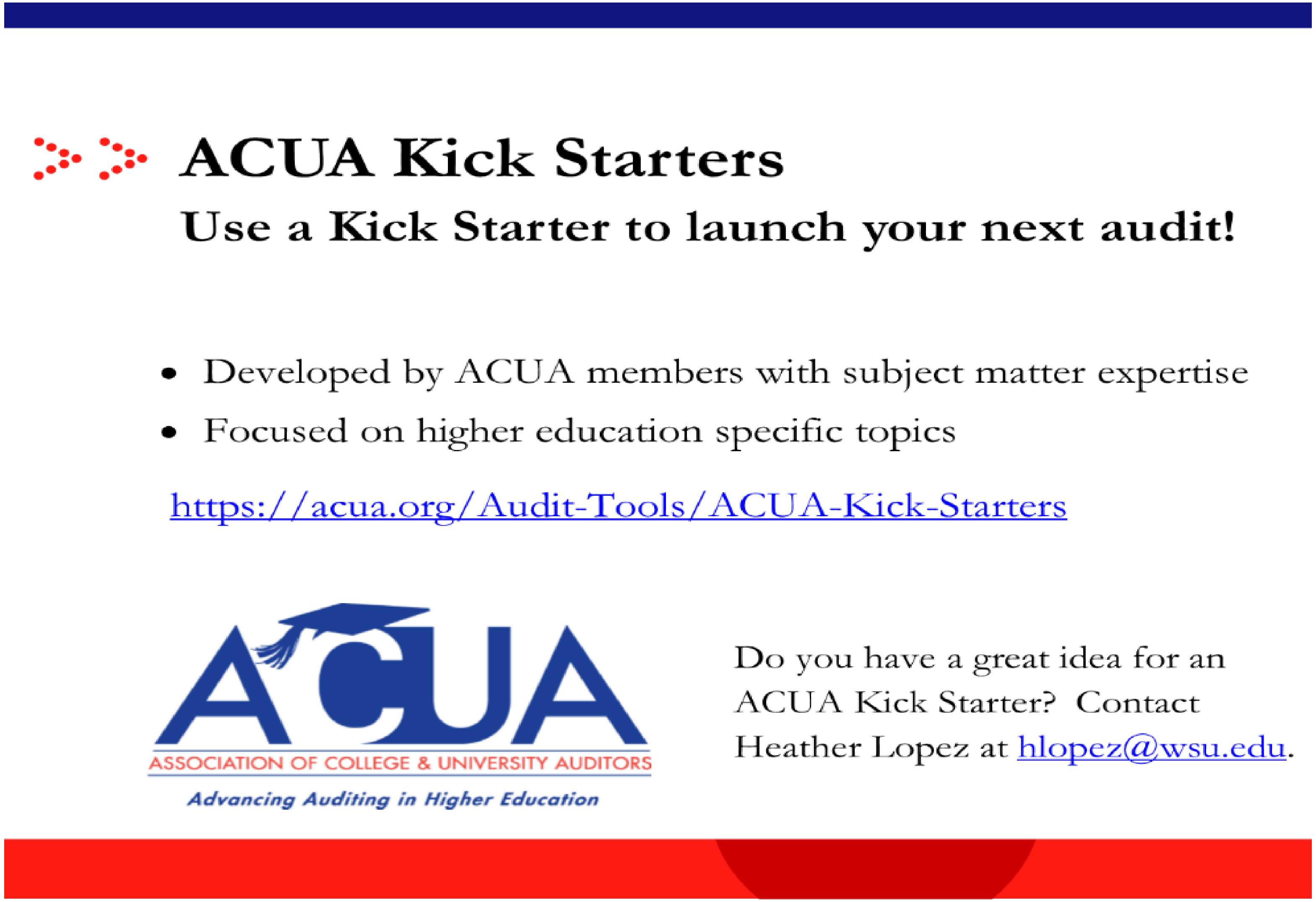
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website?

For more details, check out the Quick Tip post on

Connect.ACUA.org

Your Higher Education Auditing Connection



ACUA Kick Starters

Use a Kick Starter to launch your next audit!

- Developed by ACUA members with subject matter expertise
- Focused on higher education specific topics

https://acua.org/Audit-Tools/ACUA-Kick-Starters

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Do you have a great idea for an ACUA Kick Starter? Contact Heather Lopez at hlopez@wsu.edu.

New Kick Starter Available!

Clery Act Compliance

Download today in the members-only section of www.ACUA.org

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

ACUA WEBINARS

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education

Stay up to Date

- The College and University Auditor is ACUA's official journal. Current and past issues are posted on the ACUA website.
- News relevant to Higher Ed internal audit is posted on the front page. Articles are also archived for your reference under the Resources/ACUA News.

Connect with us

f 🐦 in You Tube

www.ACUA.org

Connect with Colleagues

- Subscribe to one or more Forums on the Connect ACUA to obtain feedback and share your insights on topics of concern to higher education internal auditors.
- Search the Membership Directory to connect with your peers.
- Share, Like, Tweet & Connect on social media.

Get Involved

- The latest Volunteer openings are posted on the front page of the website.
- Visit the listing of Committee Chairs to learn about the various areas where you might participate.
- Nominate one of your colleagues for an ACUA annual award.
- Submit a conference proposal.
- Present a webinar.
- Write an article for the C&U Auditor.
- Become a Mentor.
- Write a Kick Starter.

Solve Problems

- Discounts and special offers from ACUA's Strategic Partners
- Utilize Kick Starters
- Risk Dictionary
- Mentorship program
- NCAA Guides
- Resource Library
- Internal Audit Awareness Tool
- Governmental Affairs Updates
- Survey Results
- Career Center......and much more.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of our upcoming conferences:

Audit Interactive
April 5 – 8, 2020
Loews Vanderbilt Hotel,
Nashville, TN

- Contact ACUA Faculty for training needs.

WEBINAR MODERATOR

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

- Don’t forget to connect with us on social media!

ACUA SOCIAL NETWORKING

f 🐦 in You Tube

ACUA Distance Learning Director
Amy L. Hughes
Director of Internal Audit
Michigan Technological University

IT Access Controls Kickstarter

October 3, 2019

Michael A. Dean, CIA, CISA, CGAP, PMP

- Principal IT Auditor at Virginia Tech Office of Audit, Risk, and Compliance
- 20 Years total audit experience
- 15 years primarily IT audit focused
- Public and private sector, internal and external audit

Session Overview

- Introductory Level
- Target Audience: Junior IT auditors, or non-IT auditors needing to perform some system work themselves.
- Learning Objectives:
    1. Assess the risks associated with access controls over IT systems

    2. Develop audit procedures for assessing access controls

    3. Evaluate the effectiveness of access controls

Polling Question 1

Does your institution have dedicated information technology personnel within your internal audit function?

A. Yes

B. No

C. Not sure

What is Access Control

IT System Access Control is a process for ensuring that only personnel who are authorized to view or edit electronic data are able to access that data. The principle of Least Privilege is the basis of IT System Access Controls. This principle states that personnel should be granted access only to the information they require in order to perform their jobs. IT System Access Controls based on least privilege are a required part of many federal and state laws and regulations, as well as organizational policies.

Key Access Control Risks

- Unauthorized access could result in data modification or corruption
- Data may be exposed, stolen, or otherwise used in a manner that is illegal, unauthorized, or damaging to the organization’s interests
- Regulatory penalties
- Organizations may not be able to identify the user ID or person performing an action taken on a system
- If you don’t control who can access and edit your data, how can you ensure its integrity?

Laws and Regulations

- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLBA)
- General Data Protection Regulation (GDPR)
- Executive Order 13556 (NIST SP-171) (Controlled Unclassified Information)
- Health Insurance Portability and Accountability Act (HIPAA)

Risk Assessment Questions

- Who has access to data?
- Why do they have access?
- What data can they access?
- How do they access the data?
- Who owns the data?
- How is access granted (and by whom)?
- What happens if the data is exposed, lost, stolen, or corrupted?
- What are the relevant legal, regulatory, and policy requirements?
- How is the data protected?

Unique Individual User IDs

- Each user should have their own unique user ID
- No shared IDs or accounts
- Shared accounts make it difficult to impossible to identify who performed an action using an information system, and therefore to establish accountability in the event of a break or error
- Test: Obtain and review a user list, review and inquire about accounts that do not appear to be assigned to an individual persons.
- On some systems (Unix/Linux) multiple administrators may have to use one administrative account. In these cases, admins should login using their individual account and perform functions using sudo.
- Also change shared passwords anytime an administrator leaves

Restrict Access Rights

- Principle of Least Privilege
- Restrict users abilities to access information and performs functions to only what they need in order to perform job function
- How restricted access is likely to reflect management’s tolerance for risk, and overall philosophy
- Administrative Rights
- Encryption
- Test: Review groups memberships, management may be able to provide reports showing what resources and functions an individual can access

Polling Question 2

To what extent does your institution rely on passwords to control access to systems and data?

A. Only use passwords

B. Passwords and another factor

C. Passwords are no longer used

D. Not sure

Default Accounts and Passwords

- In most cases, should be changed, removed, or disabled
- Account names, and in some cases, passwords can be easily found by searching the internet
- If default accounts and passwords are as the vendor configured them, very easy to get into
- Test: Obtain and review a user list. Automated scanning tools can help.

Enforce Password Controls

- Passwords should be of adequate length based on organizational policies
- Passwords should enforce complexity requirements based on organizational policies
- Passwords should not be easy to guess (“password”, “12345678”, dictionary words, etc.)
- Enforce expiration and lockout for login failures based on organizational policies
- For some organizations and data risk levels, passwords may not be an adequate means of protecting accounts, and 2-factor authentication or other enhanced means of access control may be used

Enforce Password Controls

- Test: Most often done through review of security settings. Depending on systems in use, can require significant research and preparation to determine how to test.
- For Windows systems, settings are available through Group Policies
- For Linux and Unix systems, will require some research into the specific variety of Unix or Linux, as well as discussions with system administrators, to determine how to test

Polling Question 3

How would characterize your institution’s approach to controlling system access?

A. Centralized
B. De-centralized
C. Hybrid approach
D. Not sure

User Provisioning Process

- Key security area is the process for granting new accounts
- Ensure that only personnel who are authorized and approved receive obtain access, and access is only to the system resources they need to perform their job duties
- May be documented through paper forms, emails, help desk tickets, or other electronic means
- Access may be tied to employment status and position via human resources systems as well

User Provisioning Process

- Test: Important to have a good understanding of audited entity's processes for user provisioning. Obtain list of users for systems of interest, with the specific system resources they can access. Obtain documentation (whether hard copy or electronic) of the approval. Review to ensure consistency
- For personnel who have access to sensitive or high risk systems where the reason for this is not clear, seek an explanation why?

User Deprovisioning

- When a user leaves an employer or a position access rights that are no longer needed should be removed timely
- What is “timely” depends on the policy of the auditee, and the risk level associated with the data
- A particularly error prone area, particularly when account termination relies on supervisors manually informing the IT department of an employee’s departure
- Linking access rights for at least a subset of systems electronically to employment status is a way to improve timely deprovisioning

User Deprovisioning

- Test: Compare user list to list of current employees. Users who are not listed as current employees require further inquiry.
- Can also compare to list of terminated employees to identify matches
- Automated procedures (Database joins, or Excel VLOOKUP, for example) can help with comparing lists

Polling Question 4

Does your institution use automated tools for consolidating, parsing, and monitoring audit logs?

A. Yes

B. No

C. Not sure

Logging and Log Monitoring

- Organization needs to monitor access and activity on their systems
- Logging can include login successes and failures, system events, access to specific files or system resources, or use of privileged system functions.
- Logs need to be monitored and reviewed
- What gets logged and how frequently logs are reviewed should be set by organizational policy based on a risk assessment.
- Most organization of any significant complexity will require electronic tools for parsing and reviewing logs to sort through the information in their logs and extract useful data.

Questions?

- Contact: Michael Dean
- Email: michad1@vt.edu

Thanks!

Upcoming ACUA Events

October 17, 2019

Climbing the ranks: Best practices for preventing fraud and misreporting in admissions and institutional data

ACUA
WEBINARS

Join us for our upcoming webinar.