

WEBINAR

Mastering Workday: Ask an Expert Series

Session: Financial Compliance and Controls for Workday Financial Management



QUICK TIPS

Zoom Webinars

Ask Questions in Q&A Box

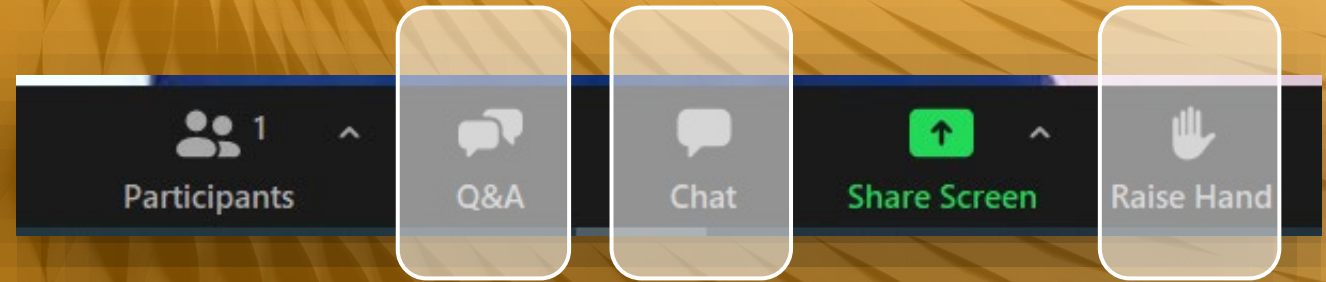
- Click the Q&A button to open the window
- Type your response in the text field
- Click Send

Chat

- Click the Chat button to open the chat panel
- Type your message in the Text box at the bottom of the panel
- Press Enter to send your message

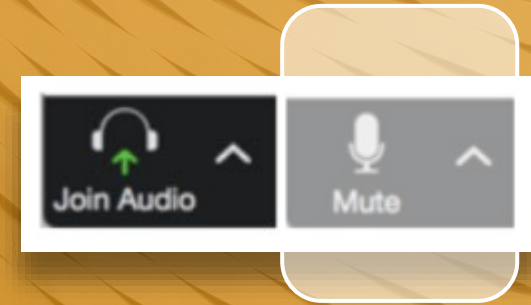
Raise Your Hand

- Click the Raise Hand button at any time to indicate to the host know that you have a question or need assistance
- To lower your hand, click the Lower Hand button



QUICK TIPS

Adjust Audio Speakers

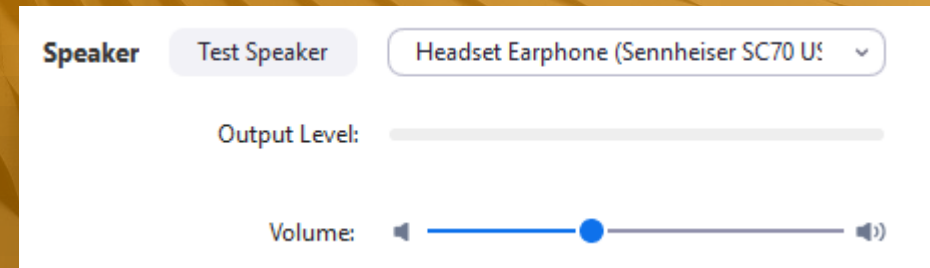


Mute | Unmute

- In the meeting controls, click the arrow next to Mute | Unmute in lower left corner

Audio Options

- Click Audio Options - this will open your audio settings
- Click Test Speaker to play a test tone
- If you cannot hear it, select a different speaker from the menu
- Try adjusting the Volume



WELCOME

Today's Expert



Justin Mitkus

Director, Consulting
Armanino

Session

Financial Compliance and Controls within Workday Financial Management

- Learn strategies for ensuring financial compliance and establishing internal controls within Workday Financial Management.
- Implement best practices for core staffing workflows in Workday with an Agile approach:
- Incorporating principals to backlogged change requests
- Evaluating cross-functional impacts and how to test effectively
- Migrating changes through well-documented production sprints

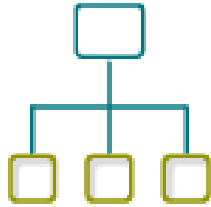
Engagement Encouraged!



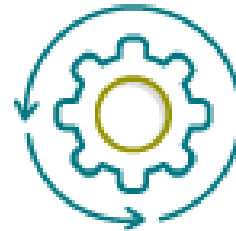
- **Interactive Q&A Sessions:** Get your specific Workday questions answered live by our experts, ensuring you leave with practical solutions tailored to your needs.
- **Expert Insights and Tips:** Gain exclusive access to professionals who will share valuable insights, tips, and best practices to enhance your Workday experience.
- **Real-World Case Studies:** Learn from real-world use cases that showcase how other organizations are successfully leveraging Workday to solve common challenges and drive business success.



Approvals



Segregation of duties



Workflows



Threshold limits

“Always-On” Audit Trail

Self-documenting electronic evidence provides pervasive audit trails-capturing who, what, and when



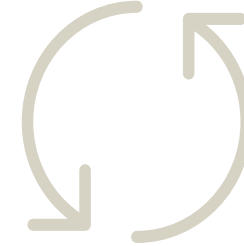
Configurable Security

- Role-based and user-based security groups
- Domain and business process policies grant permission to specific tasks and reports



Custom Validations

- Logic to require or prevent field entry
- Critical stop versus Warning alert



Business Processes

- Approval steps with configurable logic
- Example: routing a journal to Controller if it exceeds a threshold

Access Controls

These controls ensure that only authorized users have access to the system and its data. This involves user authentication, authorization, and periodic reviews of access rights to prevent unauthorized access.

Data Security Controls

These controls focus on protecting the confidentiality, integrity, and availability of data within the enterprise systems. This includes encryption, data masking, data loss prevention measures, and regular data backups.

Change Management Controls

Change management controls govern the process of making changes to the enterprise systems, such as software updates, patches, or configuration changes. Proper change management procedures help prevent unauthorized or unintended changes that could disrupt operations or compromise security.

Incident Response and Management

These controls establish procedures for detecting, responding to, and mitigating security incidents or breaches within the enterprise systems. This includes incident detection tools, incident response plans, and post-incident analysis to prevent similar incidents in the future.

Segregation of Duties

Segregation of duties controls ensures that critical tasks within the enterprise systems are divided among different individuals or roles to prevent fraud, errors, or unauthorized actions. This helps maintain accountability and reduces the risk of internal threats.

Monitoring and Logging

Monitoring and logging controls involve the continuous monitoring of system activities and the logging of relevant events for auditing and analysis purposes. This helps detect suspicious activities, track user actions, and facilitate forensic investigations in case of security incidents.

Compliance and Regulatory Controls

These controls ensure that the enterprise systems comply with relevant laws, regulations, and industry standards pertaining to data privacy, security, and governance. This includes regular audits, assessments, and adherence to standards such as GDPR, HIPAA, or PCI DSS.

Business Continuity and Disaster Recovery

Business continuity and disaster recovery controls focus on maintaining the availability of critical systems and data in the event of disruptions, such as natural disasters, cyber-attacks, or hardware failures. This involves implementing backup systems, redundancy measures, and recovery plans to minimize downtime and data loss.

Thank you for
attending

Additional Questions?

Reach out to us at

Experts@armaninio.com

