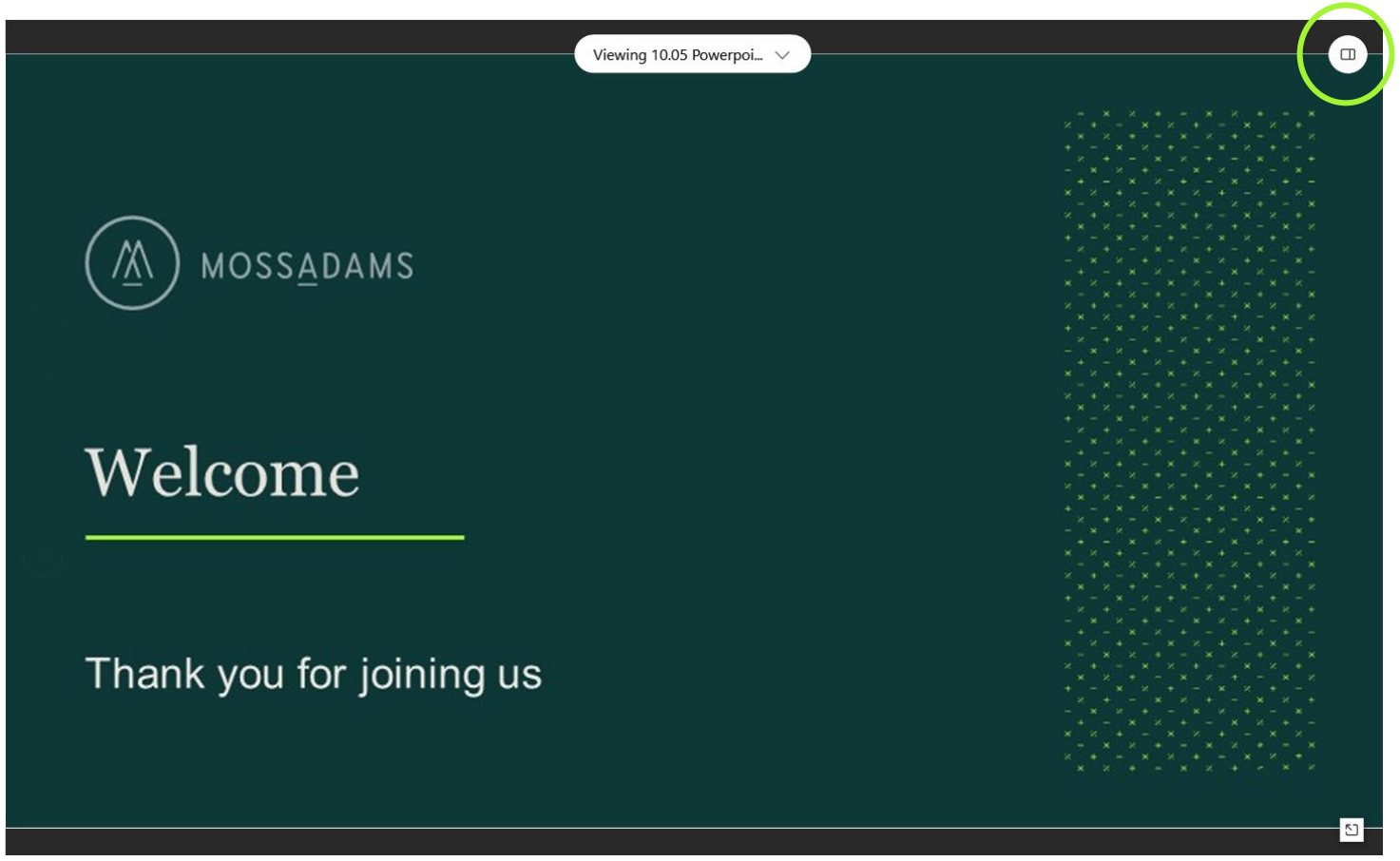
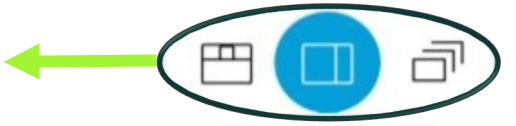
MOSSADAMS

Welcome

Thank you for joining us

Viewing Options





For optimal viewing select “Side by Side” view from the top right-hand corner.

FOR BETTER VIEWING

- Close all other applications
- Turn up your speaker volume

WebEx Controls

Mute
(not active)

Share
(not active)

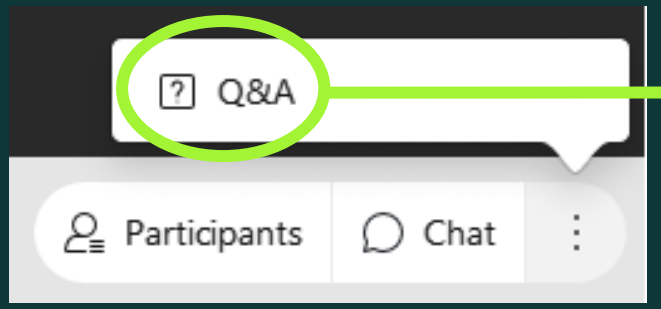
Leave

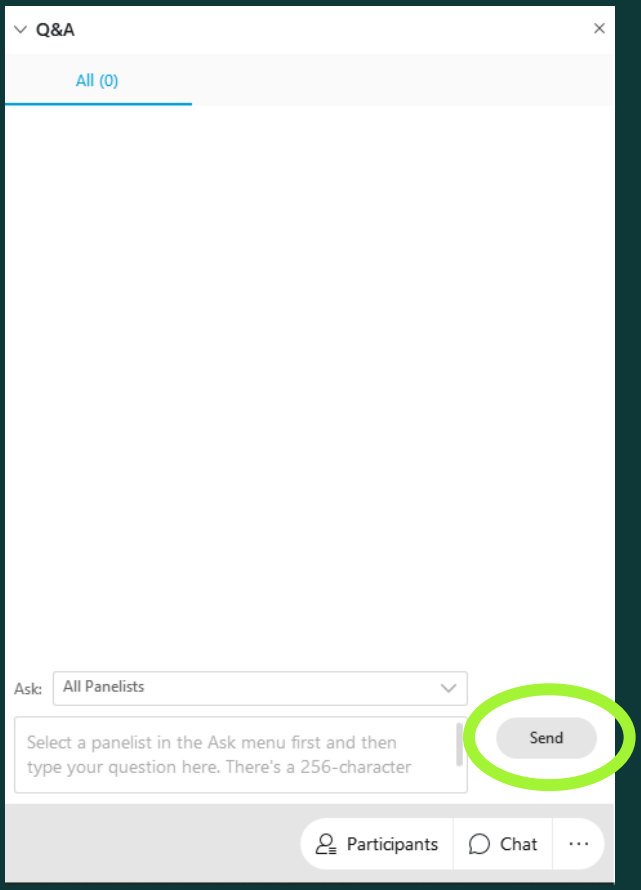
Participants

Message

More
options

Questions?





- Under the “more options” button, select “Q&A”
- A new box will open on the right-hand side to type your question to the speakers or host

Technical Difficulties?

REFRESH YOUR BROWSER BY CLICKING F5.

If you are still experiencing issues, please feel free to use the question box and direct your question to the “host”

OR

email meetings@mossadams.com

The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC.

MOSSADAMS

What to Know about Emerging SOC 2 Software Programs

September 2021

Presenters

Chris Kradjan, CPA, CITP, CRISC, HITRUST CCSFP
Managing Partner
Risk Advisory & Compliance

chris.kradjan@mossadams.com
(415) 677-8343

Maria Braun, CISA, HITRUST CCSFP
Senior Manager

maria.braun@mossadams.com
(206) 302-6295

Bryan Schader, CISSP, CISA, CHQP, CCSFP
Partner

bryan.schader@mossadams.com
(408) 558-3231

Presenters

Kevin Abbott, CISA, CISSP, PCI QSA
Partner

kevin.abbott@mossadams.com
(801) 907-4347

Bosco Yuen, CPA, CISA, CISSP, CSX, CCSA, PMP
Managing Director

bosco.yuen@mossadams.com
(310) 418-1234

Agenda

01 **SOC 2**
New market, common platforms, functionality

02 **BENEFITS AND LIMITATIONS**

03 **STANDARDS AND RESPONSIBILITIES**
AICPA standards, service auditor and organization responsibilities

04 **SELECTION CONSIDERATIONS**

The New SOC 2 Software Market

The new SOC 2 software market introduces a new breadth of functionality and scope for SaaS providers.

WHAT IT IS

SaaS solutions designed to help improve the SOC 2 audit experience for service organizations.

HOW IT WORKS

These new tools are similar to traditional GRC systems, document portals, and integrating monitoring systems.

WHAT'S CHANGED

It's a new market in its early infancy—and has significant capabilities. However, at present, it's limited in achieving its full potential.

BEST PRACTICES

It's best to gain a full understanding of its current capabilities and limitations and to be aware of added complexities and audit responsibilities for both the service organization and auditor.

Common Platforms

The following platforms offer a wide array of SOC 2 audit assistance. Due to the diverse spectrum of product focus, features, and support; carefully evaluate the tool offerings that best fit your individual needs.

COMPANIES WITH A SOC 2 AUDIT PROGRAM OFFERING:

- Apptega
- DivvyCloud
- Drata
- Fieldguide Software
- Hyperproof
- JupiterOne
- Laika
- Logicgate
- Resolver
- Secureframe
- Shujinko
- StandardFusion
- Strike Graph
- Tugboat Logic
- TruOps
- Vanta
- Very Good Security
- ZenGRC

SOC 2 Tool Functionality

Functionality and scope vary considerably by vendor.

The following are features typically advertised in SOC 2 product offerings:

AUTOMATION

- Automated evidence collection (AWS, Azure, Google Cloud, GitHub)
- Self-monitoring tool
- Document repository generator
- Standardized set of SOC 2 controls/risks

INTEGRATION

- Pre-configuration integration
- Security framework alignment and control mapping
- Gap assessment
- Policy and procedures development
- Compliance dashboards

MANAGEMENT

- Workflow management
- Security questionnaire management
- Risk register management
- Vendor risk management
- Security awareness training

Potential Benefits

These new software tools can help your service organization streamline its preparation for its first SOC audit, which could result in greater time and cost savings.

- Enable organized and efficient data collection, occasionally, without any additional time/effort from the service organization
- Provide templatized readiness assessment, controls, risk assessment, and policies
- Aggregate evidence across sources such as AWS, Azure, Google Cloud, GitHub, Jira, etc.
- Provide management with near real-time monitoring of control status through continual automated testing
- Discover areas of SOC 2 alignment with other security compliance activities such as NIST, ISO, and others
- Build an audit trail in support of audit activities
- Establish a data exchange and communication portal between the service organization and service auditor
- Access evidence previously provided to the service auditor to be used as a reference

Possible Limitations

It’s important to understand where program limitations exist. Users in a customized environment may discover difficulties when attempting to conform to a standardized solution.

SOC 2 SOFTWARE WON'T HELP YOU:

- Evaluate vulnerabilities with segregation of duties
- Consider the complexity of the service organization’s environment or structure
- Identify the system components in scope
- Assess the service organization’s market offering or industry
- Account for unique elements of security exposure
- Customize your risk analysis
- Tailor your controls
- Aggregate the data it doesn’t have links to, collecting evidence that may not be needed for the audit
- Scale as your organization matures and each business unit implements its own business requirements

Additionally, it can force the auditor to rely on the compliance platform’s development of integration between the platform and commonly used tools, regardless of the quality of your SOC report or your validation of the completeness and accuracy of the data that is pulled via the integration.

Adoption Challenges

Not all key stakeholders within the service organization may be willing to adopt the use of the SOC tool product.

- Susceptible to tacit knowledge loss in the event of system administrator or user turnover at the service organization
- Service organizations might rely on the SOC 2 compliance platform provider versus owning the tool implementation and control design and operation
- Can create added overhead for internal staff to care and feed the product
- Requires product training for each control owner and user
- Create a false sense of confidence in controls or processes that are not designed securely
- Can over-engineer evidence collection

Service Organization Responsibilities

To avoid placing excess reliance on the SOC 2 tool and its results, properly balance your organization's responsibilities with the capabilities of the program.

Tool Selection Considerations

Assess your needs, vet potential vendors, finalize your contract, and manage implementation to make sure you end up with the right software and support for your needs.

- Assess whether the system produces standardized controls based on illustrative controls or if it's tailored specific to full risks and technologies in use by the service organization
- Evaluate if the available policies and procedures are templatized versus tailored to the service organization
- Understand the workflows in place to collect information for management to review, and how auditors can extract evidence
- Determine how evidence generated and records maintained outside the SOC 2 tool can be organized and managed by the service organization
- Consider licensing obligations from the SOC 2 provider and the cost implications of this when undergoing SOC examinations
- Beware of representation of "SOC in a box" and potential for "robosigners"

Vendor Selection Considerations

Selecting the right vendor for your needs can help you overcome some pain points when transitioning to a new program.

ASSESS

the extent the vendor will help setup product and the ongoing requirements

DETERMINE

if the vendor offers training and to foster greater adoption and use of the SOC 2 tool

UNDERSTAND

if the SOC 2 tool provider offers customization necessary for the service organization

OBTAIN

references for other technology companies of similar and larger size that have used the product

Service Auditor Responsibilities

These SOC 2 software tools in no way lessen or eliminate the responsibilities of the service auditor as defined in the SOC 2 Guide and professional standards.

- Require that the service organization take responsibility for subject matter under audit before accepting the engagement
- Maintain independence from the SOC 2 tool provider
- Understand functionality and configuration of how the tool is set up for a given service organization
- Review the design of reported controls for completeness and relevance and to see that all key risks to the system are addressed
- Check if the risk assessment, policies, procedures, and other canned output have been fully tailored to fit the service organization
- Management should take responsibility to own and operate the controls under audit and data collected within the SOC 2 tool
- Check the completeness and accuracy of the information collected and reported from the tool
- Continue to perform all responsibilities defined in the SOC audit guide and AICPA Code of Professional Standards

AICPA Professional Standards

Adhere to the obligation for maintaining high ethical standards and the need to exercise due care in service delivery.

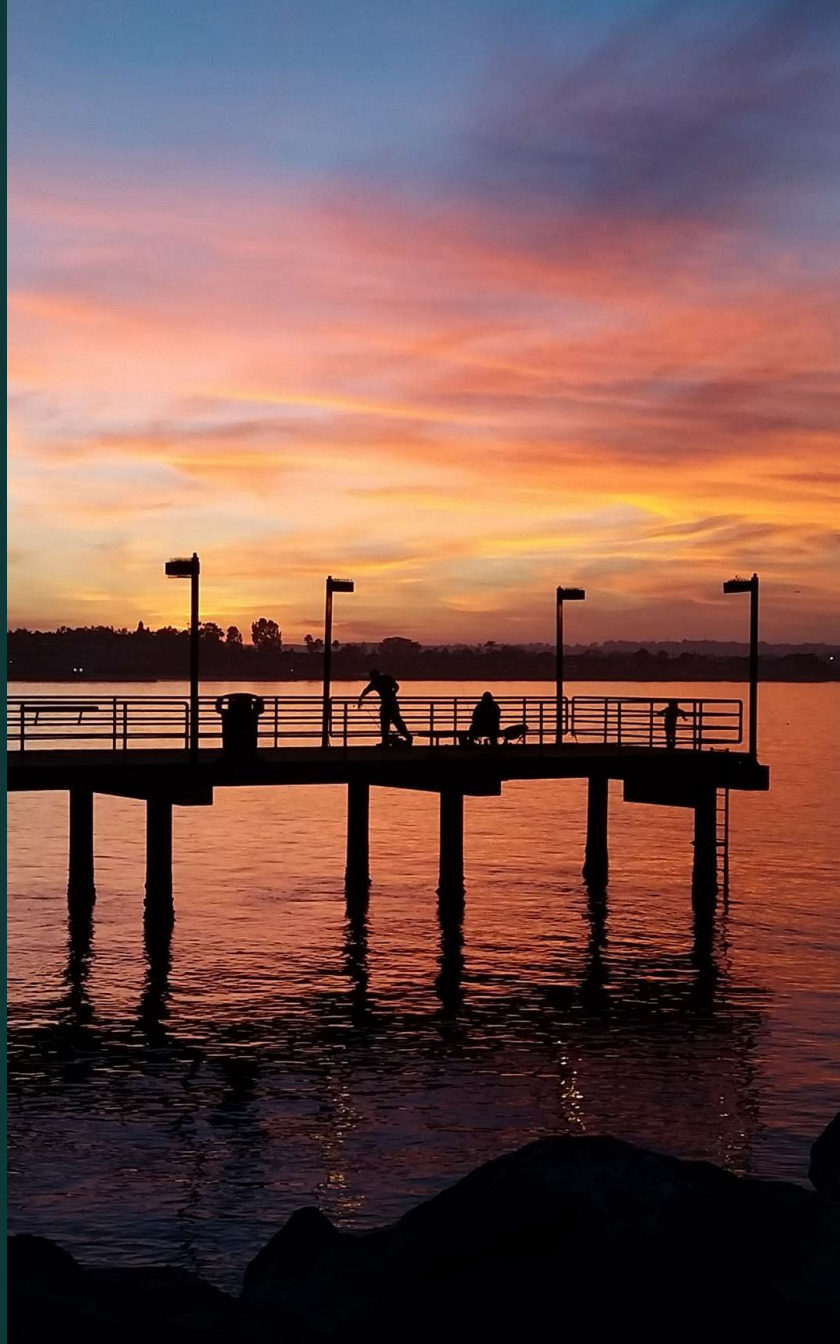
BEST PRACTICES TO FULFILL YOUR SOC 2 REQUIREMENTS:

- Operate under requirements of AICPA SOC 2 Guide and professional standards
- Follow professional responsibilities for the service auditor
- Maintain independence in fact and appearance with respect to service organization, SOC 2 tool provider, and other subservice organizations and in any matters that may threaten the performance of the SOC 2 examination
- Avoid assuming management responsibilities, review of own work, conflicts of interest, advocacy threats, and advertising or other forms of solicitation
- Implement necessary independence safeguards and decline/discontinue professional services when not possible

QUESTIONS

Let’s start a conversation.

chris.kradjan@mossadams.com
maria.braun@mossadams.com
bryan.schader@mossadams.com
kevin.abbott@mossadams.com
bosco.yuen@mossadams.com



The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Investment advisory offered through Moss Adams Wealth Advisors LLC.

THANK YOU