A Comprehensive & Adaptive Approach to SOC Compliance

The webinar presentation will begin in a few moments

NOTE: Participants will receive an email within 48 hours with a link to the slide deck and recording.

About the Presenters

Liam Collins

Partner, Armanino LLP

- Leads the firm's service organization control (SOC) and HiTrust practice
- 16+ years of SOC experience in both the audit and consulting practice areas
- Served as a Managing director at KPMG
- Has held audit, assurance, finance and IT leadership roles at PricewaterhouseCoopers, ControlMetric and Prodapt
- BSc. in accounting from Golden Gate University
- JD from the University of San Francisco School of Law
- MBA from the University of Pennsylvania's Wharton School
- Member of the American Institute of CPAs and ISACA

About the Presenters

JT Giri

CEO, nClouds

- JT co-founded nClouds to drive cloud adoption and help companies build and maintain modern infrastructures.
- 10+ years DevOps consulting experience helping solve complex operations challenges for numerous Silicon Valley-based startups.
- Deep technical skills in cloud computing infrastructure, cloud platforms, agile methodologies, and popular tools and practices for continuous integration and continuous delivery.

armanino

About the Presenters

Mike Campi

Manager, Armanino LLP

- 12+ years in financial services and accounting sector
- Helps numerous nonprofits and private schools address their tax, audit and outsourced accounting needs
- Helps CFOs determine best accounting service to support their strategic and compliance needs
- Graduate of California State University-Chico

Learning Objectives

During today's webinar, we will:

- Review why change management is important when implementing cloud solutions
- Discuss real life examples of how effective change management can support a comprehensive and adaptive approach to SOC compliance
- Outline recent changes to SOC I and upcoming changes to SOC II compliance requirements

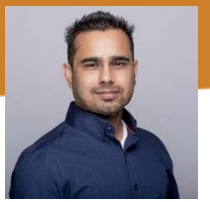
Polling Question #1

Change Management

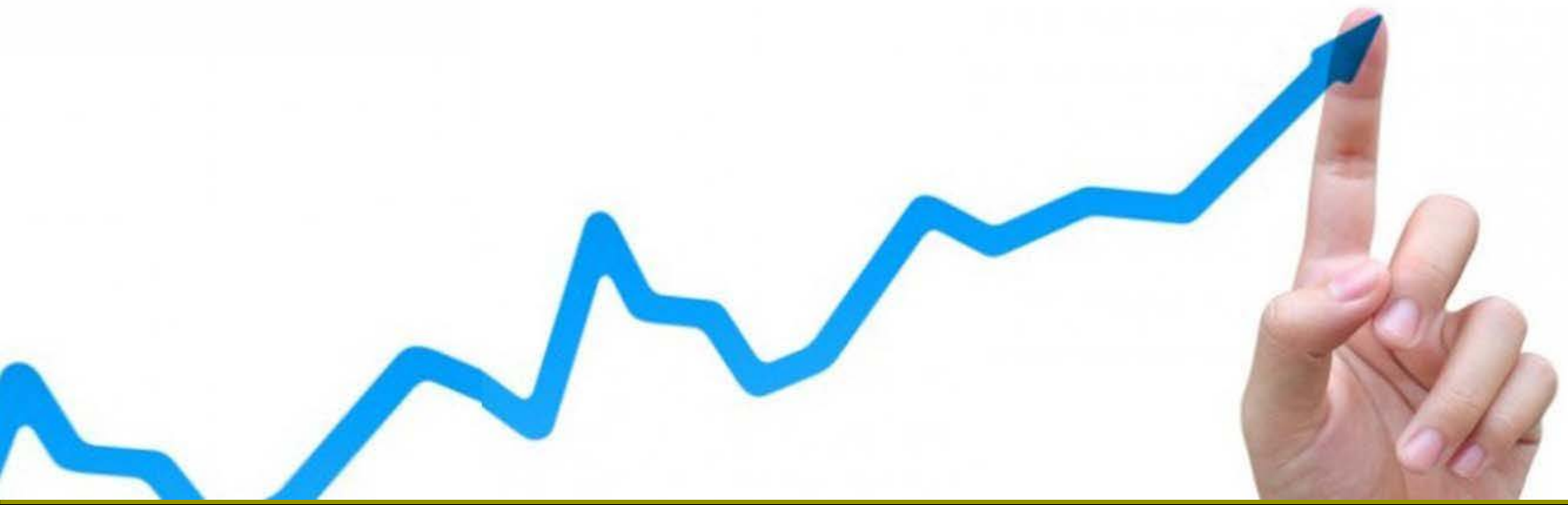
Cloud Advantages

- Fast provisioning
- Infrastructure as a code
- Elasticity
- Multiple regions and availability zones

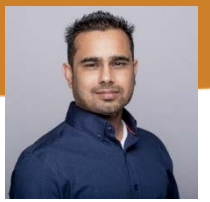
Dynamic Environment



- Number of resources = 100x
- Number of people making changes = 10-100x
- Number of people in operations = Same as before



Infrastructure Tools



Terraform

CloudFormation

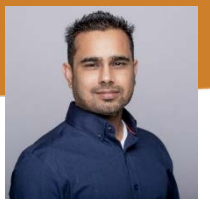
Ansible

Continuous Delivery

armanino

Polling Question #2

Unique Challenges of Cloud



- SOC audits
- Compliance audits
- Underutilized resources

armanino

Why is Change Management Important in Cloud?

- Currently, change management is accomplished by sharing spreadsheets, consuming tremendous amounts of time, especially if you are going through an SOC audit.
- Without a proper change management process, resources continue to skyrocket.
- The best approach to maintain costs and stay secure is in the cloud.

armanino

Polling Question #3

Change Management Best Practices

- Establish strong policies
- Automate approval process
- Trace back every change to JIRA or any other ticketing system.

armanino

nOps Rules

nOps Dashboard

Secure https://uat.nops.io/v2/changes/nops_rule

nOps | AWS Resources | Change management | Event log | Search for resources.. | admin

Changes Summary | nOps Rules | Reports

nOps Rules

Applied nOps Rules | Available nOps Rules

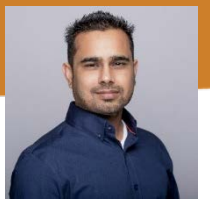
Below is the list of all applied nOps rules on your aws projects and resources

Add More nOps Rules

Rule Name	Project	Region	Cost	Compliance
CloudTrail Check	--	--	--	Compliant
Dynamodb Throughput Check	--	--	--	Compliant
Inactive access keys Check	nOps-UAT, nops-child-account, nOpsRole, ChildAccountWithoutBilling	--	--	10 non-compliant resources
Resource Limits Check	nOps-UAT	--	--	4 non-compliant resources
Root Account MFA Check	nOpsRole, nops-child-account, ChildAccountWithoutBilling	--	--	3 non-compliant resources
Tag Violation Check	nOps-UAT	us-east-1, us-west-2	795.96	20 non-compliant resources

armanino

JIRA Workflow Integration



JIRA
Workflow Integration

nOps Dashboard
Secure https://uat.nops.io/v2/changes
nOps AWS Resources Change management Event log
Changes Summary nOps Rules Reports
Change Management (Active)
Jul 17 2017 4:56:02 PM - Jul 24 2017 4:56:02 PM
Date Project Event Name IAM Users IAM Roles Status
1w Active
Open (7) Approved (2) All (9)
Showing All changes
Select all Create jira tickets
i-09fa63c0a0463c513 invoked RevokeSecurityGroupIngress api
Last Created on: 4 days ago | Cost: N/A | Project: nOps-UAT
1 active resources 1 events
i-09fa63c0a0463c513 invoked AuthorizeSecurityGroupIngress api
Last Created on: 4 days ago | Cost: N/A | Project: nOps-UAT
1 active resources 1 events

armanino

User Changes

Create Jira Issues

Issue Types Select Issue Type * Select Issue Type

Jira Project Select Jira Project * Select Project

Jira Summary

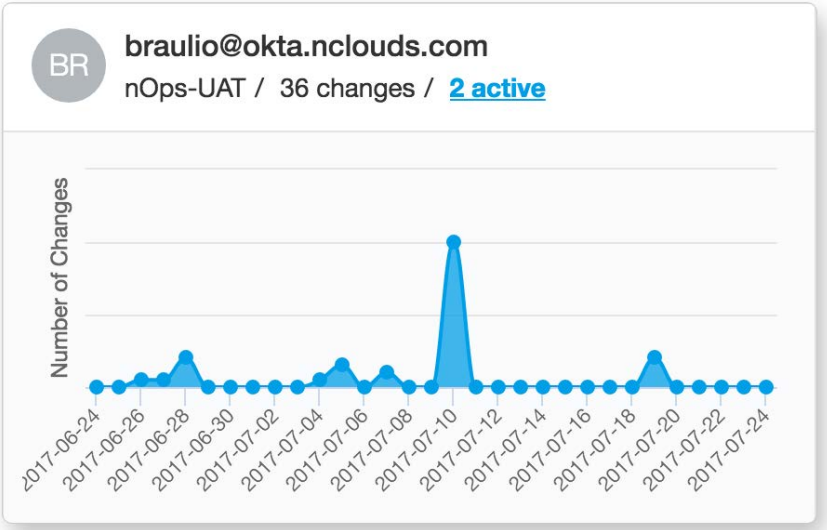
* Summary is required

Jira Description

i-09fa63c0a0463c513 invoked AuthorizeSecurityGroupIngress api in region us-west-2
http://uat.nops.io/v2/changes/detail/129206

Create Issue | Cancel

- **Track changes made by user**



armanino

Polling Question #4

SOC Update

SOC 2 Updates

- Renames *Trust Services Principles and Criteria* as simply *Trust Services Criteria*
- Restructures and aligns the trust services criteria with the COSO 2013 framework to facilitate their use in an entity-wide engagement
- This restructuring added criteria that had not been required in prior SOC 2 audits
- Developed a SOC for Cybersecurity reporting option and associated criteria
- SOC2+ - service organization may request that the auditor's report address additional subject matter related to the service organization's services such as:
  - Reporting on the historical availability of data
  - Compliance with a statement of privacy practices
  - HIPAA compliance

armanino

SOC 2 Update – Added Criteria

Area	Additional Focus Areas
Board of Directors	Accepts oversight responsibilities Ensures appropriate skills to hold management accountable Maintains independence
Information to support internal control	Obtains and processing appropriate information to support internal controls Captures and processes relevant data into information
Risk Assessment	Identifies and assesses risk related to the achievement of objectives: • Operations • External financial reporting • External nonfinancial reporting • Internal reporting • Compliance • Fraud
Assessment of changes that can impact internal controls	Assess the impact of changes in: • Business modal • Leadership • Systems and technology • External environment • Vendor and business partner relationships
Develop risk mitigation activities for risks arising from potential business disruptions	Polices and solutions to respond, mitigate and recover from security incidents that disrupt business operations Use of insurance to mitigate financial impact risks

armanino

SSAE 18 Updates

The more significant revisions to the attestation standard directly affecting SOC audits and reports, impacting SOC 1 reports issued after May 1st, 2017:

Complementary subservice organization controls	Management is required to identify controls that management assumes will be implemented by those subservice organizations and that are necessary to achieve the control objectives stated in management's description. Management must also link to the relevant control objectives impacted.
Risk Assessment	Additional risk assessment context is provided for the service auditor around understanding the service organization's system and understanding the risks and assessment of material misstatements. Management should also assess the design of their controls and have this documentation available for auditor review.
Completeness & Accuracy	Reinforcement of the service auditor's requirement to evaluate evidence around the completeness and accuracy of information produced by the service organization
Complementary user entity controls	Reinforces that Complementary User Entity Controls (CUEC's) should only include controls that are necessary to achieve the control objectives stated in management's description.
Review of Internal Audit reports	Service auditors will be required to review internal audit reports and regulatory examinations relating to the services provided to user entities and the scope of the report.

armanino

SOC for Cybersecurity

- Demand for an attestation report covering an entity's cybersecurity risk management program promoted action by the AICPA
- No carve-out for subservice providers
- Regulatory Focus – Effective March 1, 2017 NY State Dept. of Financial Services now requiring banks, insurance companies etc. to submit a certification of compliance
- Description criteria have been developed to guide management's description of their cybersecurity program
- Control criteria have been developed for auditors to perform the attestation
- Report includes:
  - Management description of the company's cybersecurity risk management program
  - Management's assertion
  - Auditor's opinion

armanino

In Conclusion

During today's webinar, we have:

- Reviewed why change management is important when implementing cloud solutions
- Discussed real life examples of how effective change management can support a comprehensive and adaptive approach to SOC compliance
- Outlined recent changes to SOC I and upcoming changes to SOC II compliance requirements

armanino

CONTACT US

Liam Collins	Audit Partner, Armanino	Liam.Collins@armaninoLLP.com
JT Giri	CEO, nClouds	JT@nOps.io
Mike Campi	Manager, Armanino	Mike.Campi@armaninoLLP.com

NOTE: Participants will receive an email within 48 hours with a link to the slide deck and recording.