Building a Successful Cloud Audit Plan: An Expansive Perspective

November 14, 2018

Matt Stamper: CISO | Executive Advisor
MPIA, MS, CISA, CISM, ITIL, CIPP-US
Building a Successful Cloud Audit Plan: An Expansive Perspective

November 14, 2018

Matt Stamper: CISO | Executive Advisor
MPIA, MS, CISA, CISM, ITIL, CIPP-US
We’re going to cover a lot of ground!

This is an open dialogue:
Your Questions are Welcomed
Agenda

- Learning Objectives
- Quick Poll
- Context Counts – Always
- Audit Scope & Objectives
- What’s Similar / What’s Changed
- ITSM & The Cloud
Learning Objectives

- **Develop**: Develop a cloud audit program that is comprehensive and repeatable.
- **Validate**: Validate privacy and security risks of cloud services to meet organizational objectives and risk tolerances.
- **Apply**: Apply professional skepticism in evaluating and assessing vendor claims relative to governance and security.
- **Include**: Include broader context of organizational objectives and strategy to the cloud services audit plan.
Quick Poll

• Who has accessed aws.amazon.com and set up an account?

• Who believes cloud services are inherently insecure?

• Who believes that when you load data / information to the cloud, it’s transferred overseas?
Context Counts

Macro: Industry, Geography, Sector, Market, Regulatory Environment

Micro: Management, Funding, Staffing Levels & Competencies, Strategy & Initiatives


Applications: SaaS, On-Premise (tied to lines of business and processes)

Infrastructure: App Code, Databases, OS, Hypervisors, Compute, Networks (SAN, Backup, WAN/LAN)

Know how each layer impacts the others
Context Counts

What should *not* go to the cloud? Why?

Macro: Industry, Geography, Sector, Market, Regulatory Environment

Micro: Management, Funding, Staffing Levels & Competencies, Strategy & Initiatives


Applications: SaaS, On-Premise (tied to lines of business and processes)

Infrastructure: App Code, Databases, OS, Hypervisors, Compute, Networks (SAN, Backup, WAN/LAN)

Know how each layer impacts the others
Context Counts

How does this broader context affect your perspective of cloud services

Macro: Industry, Geography, Sector, Market, Regulatory Environment

Micro: Management, Funding, Staffing Levels & Competencies, Strategy & Initiatives


Applications: SaaS, On-Premise (tied to lines of business and processes)

Infrastructure: App Code, Databases, OS, Hypervisors, Compute, Networks (SAN, Backup, WAN/LAN)
Typical Audit Plan
Audit Plans

Audit Objectives
- Policy Procedures
- Internal Controls
- Regulatory Requirements
- Vendor Management Requirements

Audit Scope
- Business Processes
- Applications
- Vendors / Cloud Provider(s)
- Functions

Testing, Evaluation of Results & Reporting
Cloud Audit Context

Some basic questions to consider when building a cloud audit plan include:

1. Is the service or application authorized to be in the cloud?
2. What is the role of the application or service?
3. What type of information or data is used by the application?
4. Do we have the right skills, competencies and staff to operate in the cloud?
5. Have risks changed given the use of cloud services be they SaaS or IaaS?
Common Cloud Risks?

What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between the provider and customer?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?
What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between the provider and customer?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?

Who has administrative control over the service or account?
Common Cloud Risks?

What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between the provider and customer?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?

How can we assess the security and appropriateness of configurations?
Common Cloud Risks?

What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration, such as S3?
3. Loss of control?
4. Asymmetries between the provider and customer?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?

How are we defining control in the context of the cloud?
Common Cloud Risks?

What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between the provider and customer?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?

Who has greater power in negotiations (T&Cs / Pricing)?
Common Cloud Risks?

What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between the provider?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?
Common Cloud Risks?

What do you believe to be the most common cloud risks?

1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between provider and customer?
5. Comingling?
6. Jurisdictional?
7. Who should make risk decisions?

How does the venue of services impact legal / compliance requirements?
Common Cloud Risks?

What do you believe to be the most common cloud risks?
1. Account lock-out / resource hijacking?
2. Misconfiguration leading to a breach (e.g. S3)?
3. Loss of control?
4. Asymmetries between the provider and customer?
5. Comingling of data / multi-tenancy?
6. Jurisdictional?
7. Who should make risk decisions?

Most critically, who is authorized to make risk decisions?
What risks do you consider most critical?
A More Expansive View...
Trust & Ethics: More Important Than We Realize
Ethics, Trust & Economics
ὁμνυμι Ἀπόλλωνα ἰητρὸν καὶ Ἀσκληπιὸν καὶ Ὑγείαν καὶ Πανάκειαν καὶ θεοὺς πάντας τε καὶ πάσας, ἵστορα
ποιεύμενος, ἐπιτελέα ποιήσειν κατὰ δύναμιν καὶ κρίσιν ἐμὴν ὄρκον τὸν τόνδε καὶ συγγραφὴν τήν
tήν:

διατήμασί τε χρήσομαι ἐπ” ώφελεὶ καὶ τέχνην κατὰ δύναμιν καὶ κρίσιν ἐμὴν, ἐπὶ δηλήσει δὲ καὶ ἀδίκε
εὑρέθησαν.

οὐ δώσω δὲ οὐδὲ φάρμακον οὐδενὶ αἰτηθεὶς θανάσιμον, οὐδὲ ὑφηγήσομαι συμβουλίην τοιὴν: ὅμοιος δὲ
οὐδὲ γυναικὶ πεσσὸν φθόριον δώσω.

ἁγνῶς δὲ καὶ ὁσίως διατηρήσω βίοντὸν καὶ τέχνην τήν ἐμὴν.

οὐ τεμέω δὲ οὐδὲ λιθιῶντας, ἐκχωρήσω δὲ ἐργάταισιν ἀνδράσι πρῆξιος τῆσδε.

ἐς οἰκίας δὲ ὅκοσας ἂν ἐσίω, ἐσελεύσομαι ἐπ” ώφελεὶ κατὰ βίον ἀνθρώπων, ἢ μὴ χρή ποτε ἐκλαλεῖσθαι
ἐξω, σιγήσομαι, ἄρρητα ἡγεύμενος εἶναι τὰ τοιαῦτα.

ὁρκον μὲν οὖν μοί τόνδε ἐπιτελέα ποιήσω, καὶ μὴ συγχέωντι, εἰ ὕπαρασθαι καὶ βιοὺ καὶ τέχνης
δοξαζόμενων παρὰ πᾶσιν ἀνθρώποις ἐς τὸν αἰεὶ χρόνον: παραβαίνοντι δὲ καὶ ἐπιορκέοντι, τάναντι
τούτων.
"If you take a broad enough definition of trust, then it would explain basically all the difference between the per capita income of the United States and Somalia," ventures Steve Knack, a senior economist at the World Bank who has been studying the economics of trust for over a decade. That suggests that trust is worth $12.4 trillion dollars a year to the U.S., which, in case you are wondering, is 99.5% of this country's income (2006 figures). If you make $40,000 a year, then $200 is down to hard work and $39,800 is down to trust.

https://www.forbes.com/2006/09/22/trust-economy-markets-tech_cx_th_06trust_0925harford.html#479dac0a2e13
Here is where we see trust in action

Take pause and think about how trust impacts your day-to-day life...
Behavioral Economics...our models change

“individuals are honest only to the extent that suits them (including their desire to please others)”

— Dan Ariely, *Predictably Irrational: The Hidden Forces That Shape Our Decisions*

Stated differently, situational ethics.
Duty of Care

This duty requires that directors inform themselves “prior to making a business decision, of all material information reasonably available to them.” Whether the directors were informed of all material information depends on the quality of the information, the advice available, and whether the directors had “sufficient opportunity to acquire knowledge concerning the problem before action.” Moreover, a director may not simply accept the information presented. Rather, the director must assess the information with a “critical eye,” so as to protect the interests of the corporations and its stockholders.

https://www.law.cornell.edu/wex/fiduciary_duty
Duty of Disclosure: This duty requires directors to act with “complete candor.” In certain circumstances, this requires the directors to disclose to the stockholders “all of the facts and circumstances” relevant to the directors’ decision.

https://www.law.cornell.edu/wex/fiduciary_duty
How do Trust, Ethics & Behavioral Economics Influence Cloud Audits?
Organizations using SaaS and other cloud services must assess risk in a valid, meaningful manner.
Security Defined

The easiest way to think about security is to think about the outcome of what good security provides: **confidentiality, integrity, and availability** of information (CIA).

**Confidentiality** is the end-state of ensuring that information is only viewed and acted upon by those individuals, organizations, or systems that are authorized to see such information. “A loss of confidentiality is the unauthorized disclosure of information” – FIPS 199.

**Integrity** is the end-state of information and its processing such that the information is believed to be complete, accurate, valid and subject to restricted access (CAVR)...essentially un tampered with or otherwise modified by unauthorized activity. “A loss of integrity is the unauthorized modification or destruction of information” – FIPS 199.

**Availability** is simply that...that the information is available for its required use without delay or loss. “A loss of availability is the disruption of access to or use of information or an information system” – FIPS 199.

Collectively, IT security is the set of processes that are involved with ensuring that data and information meet the confidentiality, integrity, and availability objectives of business.
Security Risk
Background

In October of 2011, the SEC’s Division of Corporate Finance offered guidance on how the risks related to cybersecurity should be disclosed by registrants – notably around topics such as the impairment of goodwill, the costs associated with addressing a security incident, and the timeliness, comprehensiveness and accuracy of such disclosures.

(CF Disclosure Guidance: Topic No. 2)

New Interpretive Guidance issued in 2018

In February, 2018, the SEC expanded upon the Division of Corporate Finance’s guidance with a more comprehensive set of expectations related to registrants addressing cybersecurity risks including a more detailed accounting of the risks of a security incident coupled with expected controls related to disclosures of cybersecurity risks and incidents and the prevention of insider trading based on the access to material, non-public information.

Focus of the SEC’s Interpretive Guidance:

• Costs of cybersecurity incidents can be “material”
  • Remediation costs
  • Increased cybersecurity protection costs
  • Lost revenues
  • Increased insurance premiums
  • Reputational damage
  • Damage to competitiveness

• Specifically, “the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.”

• Definition of Materiality: “...there is a substantial likelihood that a reasonable investor would attach importance in determining whether to buy or sell the securities registered.”
SEC Expectations:

• “First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents.”

• “Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents.”
Guidance on Reporting & Disclosures

- Cybersecurity risks should be adequately disclosed in Periodic Reports (e.g. 10-Q, 10-K or 20-F) and specifically captured in the following sections of these reports:
  - Business & Operations
  - Risk Factors
  - Legal Procedures
  - Management’s Discussion and Analysis (MD&A)
  - Financial Statement Disclosures

- Changes, including incidents, should be timely disclosed in Current Reports (e.g. 8-K, 6-K)

- There is an explicit duty to correct prior disclosures that were incomplete or inaccurate

- The SEC also warns against providing “boilerplate” disclosures that do not capture the organization’s context and adequately communicate the nature and extent of its security program
Risks the SEC expects to be evaluated:

- Materiality of incidents (nature, extent and potential magnitude)
- *Previous security incidents / probability of future events based on the status of the current cybersecurity program*
- *Adequacy of preventative actions and their costs*
- Analysis of “harm” that could impact the registrant including impacts to:
  - Company reputation
  - Financial performance
  - Customer and vendor relationships
  - Litigation
  - Regulatory investigations
The Role of the Board of Directors

The SEC clearly expects the board to be both informed and to exercise appropriate oversight related to cybersecurity risks.

“Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors’ role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board’s leadership structure.”

“A company must include a description of how the board administers its risk oversight function.”
Key Takeaways from the SEC Guidance

• The Board of Directors has a fiduciary role in overseeing cybersecurity risk

• Executive management needs to adequately understand the materiality of the registrant’s cybersecurity program

• CISOs should proactively communicate cybersecurity risks and changes to their cybersecurity program to inform required disclosures

• Registrants need adequate controls over both cybersecurity risk and controls over insider trading based on material, non-public information related to cybersecurity incidents
Auditors need to understand service demarcation and basic ITIL functions.
Services by Layer: Security is Foundational

Service Demarcation:
Contracted SLAs, SLOs, Roles & Responsibilities

On Site
- Applications
- Database
- O/S
- Hypervisors
- Servers
- Storage
- Networks
- Backups

Infrastructure (as a Service)
- Applications
- Database
- O/S
- Hypervisors
- Servers
- Storage
- Networks
- Backups

Platform (as a Service)
- Applications
- Database
- O/S
- Hypervisors
- Servers
- Storage
- Networks
- Backups

Software (as a Service)
- Applications
- Database
- O/S
- Hypervisors
- Servers
- Storage
- Networks
- Backups

Security, Monitoring & Governance: Critical Foundation
### Services by Layer: Security is Foundational

#### Service Demarcation:
**Contracted SLAs, SLOs, Roles & Responsibilities**

<table>
<thead>
<tr>
<th>Layer</th>
<th>On Site</th>
<th>Infrastructure (as a Service)</th>
<th>Platform (as a Service)</th>
<th>Software (as a Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Database</td>
<td></td>
<td>Database</td>
<td>Database</td>
<td>Database</td>
</tr>
<tr>
<td>O/S</td>
<td></td>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
</tr>
<tr>
<td>Hypervisors</td>
<td></td>
<td>Hypervisors</td>
<td>Hypervisors</td>
<td>Hypervisors</td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td></td>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td>Networks</td>
<td>Networks</td>
<td>Networks</td>
</tr>
<tr>
<td>Backups</td>
<td></td>
<td>Backups</td>
<td>Backups</td>
<td>Backups</td>
</tr>
</tbody>
</table>

---

**Who is responsible for a data breach?**

- **Client**
- **Cloud Provider**

---

**Security, Monitoring & Governance: Critical Foundation**
## Services by Layer: Security is Foundational

### Service Demarcation: Contracted SLAs, SLOs, Roles & Responsibilities

<table>
<thead>
<tr>
<th>On Site</th>
<th>Infrastructure (as a Service)</th>
<th>Platform (as a Service)</th>
<th>Software (as a Service)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Database</td>
<td>Database</td>
<td>Database</td>
<td>Database</td>
</tr>
<tr>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
</tr>
<tr>
<td>Hypervisors</td>
<td>Hypervisors</td>
<td>Hypervisors</td>
<td>Hypervisors</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networks</td>
<td>Networks</td>
<td>Networks</td>
<td>Networks</td>
</tr>
<tr>
<td>Backups</td>
<td>Backups</td>
<td>Backups</td>
<td>Backups</td>
</tr>
</tbody>
</table>

**Security, Monitoring & Governance: Critical Foundation**

**How are roles & responsibilities defined?**

[Diagram showing service demarcation]

---

*(Note: The diagram visually represents the demarcation of services and responsibilities across different layers.)*

---

*(End Note)*
# Key Functions for IT

## IT Infrastructure (Holistic View)

### IT Infrastructure:
- Application
- Database
- Operating System
- Hypervisor
- Servers
- Networks:
  - Storage
  - IP
  - Backup
  - Administration
- Data Center

### 3rd-Party Services:
- Risk Management
- Vendor Assessment
- Business Associate Agreements (HIPAA)
- Financial
- Contracts
- Cloud Service Providers
- SaaS Applications

### IT Service Management:
- Change Management
- Incident Management
- Configuration Management
- Data Management
- Risk Management
- Availability Management

---

### Security, Monitoring & Governance: Critical Foundation
Questions relative to Cloud Services:

- How do I evaluate change management in the cloud – notably with ephemeral services?
- How do I handle security incidents that involve my cloud provider:
  - Forensics
  - Data breaches
  - Logs
- How do I evaluate security configurations in the cloud, notably with SaaS services?
- How do I inventory assets in the cloud?
- How do I verify the location of my services?
Vendor Management

Cloud Services are inextricably linked to vendor management practices. Service demarcation is key.
Categories of Vendor Risk:

- Financial
  - Considerations: Viability, Stability

- Operational
  - Considerations: Performance, Security

- Compliance
  - Considerations: Legal, Regulatory

- Strategic
  - Considerations: Strategy, Fulfillment

- Geographic
  - Considerations: Geopolitical, Cultural

Essentially, how can we triage and contextualize vendor risk effectively?
Vendor-Focused Risk Register

Consider the use of a vendor-focused risk register. The risk register should incorporate the following elements:

- Impacts
- Likelihood
- Materiality of the relationship
- Category of risk
- Accountabilities
Focus on Materiality

Develop a materiality matrix that evaluates cloud services in the context of their impact on the following:

- Privacy
- System Availability
- Financial Exposure
- Organizational Reputational
- Protected Information (e.g. PHI, Personal Data, Payment Card)
Incident Management

Incident management is fundamentally different in the Cloud.
Incident Response is Different in the Cloud

<table>
<thead>
<tr>
<th>Policy Procedures Runbooks</th>
<th>Breach Notification(s)</th>
<th>Coordination between departments</th>
<th>Conflicting Priorities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Engagement with Law Enforcement</td>
<td>Distraction and business impact</td>
<td>Third-Parties</td>
</tr>
<tr>
<td></td>
<td>Log Review Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forensics</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Investigate Headers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malware Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TTPs Threat Intel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Activities below the line are largely technical in nature and require specialized skills but equally important above the line context.
Let’s Look at AWS
Which Region(s)?

How does this impact your audit?
Which Services?

The most common services are EC2, S3, S3 Glacier but there are hundreds ... each with unique configurations.
IAM controls can be placed on objects & users.
Many of the items can be set up in Cloud Trail to inform your audit.
EC2 Instance Types

Step 1: Choose an Amazon Machine Image (AMI)

Quick Start

- My AMIs
- AWS Marketplace
- Community AMIs

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-061e7ebbc234015fe
  - Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glib 2.56, Binutils 2.29.1, and the latest software packages through extras.
  - Root device type: ebs
  - Virtualization type: hvm
  - ENA Enabled: Yes
  - Select
  - 64-bit (x86)

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-a0dcf6ed8
  - The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
  - Root device type: ebs
  - Virtualization type: hvm
  - ENA Enabled: Yes
  - Select
  - 64-bit (x86)

Red Hat Enterprise Linux 7.5 (HVM), SSD Volume Type - ami-28e07e650
  - Select

- Feedback
- English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy | Terms of Use

Type here to search
Compute: Tags Can Be Used for Audit Purposes
# Logs & Audit Tools?

Welcome to CloudTrail

With CloudTrail, you can view events for your AWS account. Create a trail to retain a record of these events. With a trail, you can also create event metrics, trigger alerts, and create event workflows. [Learn more](#)

## Create trail

### Recent events

These are the most recent events recorded by CloudTrail. To view all events for the last 90 days, go to Event history.

<table>
<thead>
<tr>
<th>Event time</th>
<th>User name</th>
<th>Event name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-11-08, 04:28:43 PM</td>
<td>root</td>
<td>DescribeSecurityGroups</td>
</tr>
<tr>
<td>2018-11-08, 04:28:20 PM</td>
<td>root</td>
<td>DescribeTags</td>
</tr>
<tr>
<td>2018-11-08, 04:28:18 PM</td>
<td>root</td>
<td>DescribeStateSecurityGroups</td>
</tr>
<tr>
<td>2018-11-08, 04:28:17 PM</td>
<td>root</td>
<td>DescribeVpcs</td>
</tr>
<tr>
<td>2018-11-08, 04:28:17 PM</td>
<td>root</td>
<td>DescribeSecurityGroups</td>
</tr>
</tbody>
</table>
Some Important Detail…

Event history

Your event history contains the activities taken by people, groups, or AWS services in supported services in your AWS account. By default, the view filters out read-only events. You can change or remove that filter, or apply other filters.

You can view the last 90 days of events. Choose an event to view more information about it. To view a complete log of your CloudTrail events, create a trail and then go to your Amazon S3 bucket or CloudWatch Logs. Learn more

<table>
<thead>
<tr>
<th>Event time</th>
<th>User name</th>
<th>Event name</th>
<th>Resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-11-08, 04:25:49 PM</td>
<td>root</td>
<td>ModifyNetworkInterfaceAttribute</td>
<td>EC2 NetworkInterface and 1 more</td>
</tr>
<tr>
<td>2018-11-08, 10:30:44 AM</td>
<td>root</td>
<td>ConsoleLogin</td>
<td></td>
</tr>
<tr>
<td>2018-11-08, 10:04:00 AM</td>
<td>root</td>
<td>ConsoleLogin</td>
<td></td>
</tr>
<tr>
<td>2018-11-08, 10:00:46 AM</td>
<td>root</td>
<td>ConsoleLogin</td>
<td></td>
</tr>
</tbody>
</table>
Leverage Native AWS Features for Budgeting

AWS Budgets

Create and manage budgets
Set custom cost and usage budgets to more easily manage your AWS spend. Monitor your budget status from the Budgets Dashboard.

Refine your budget using filters
Track your cost or usage across multiple dimensions by adding filters related to Service, Linked Account(s), Availability Zone, and more.

Add notifications to your budget
Set up to five alert thresholds for each budget. Each alert can notify up to ten email recipients as well as publish updates to an Amazon SNS topic of your choice.

For more information, refer to the Managing Your Costs With Budgets section in the AWS Billing & Cost Management user guide.
Tags are Great Tools
Firewalls Have Changed
Security Groups

This is just an example 😊
Simple Storage Service (S3) – AKA a “Bucket”
Simple Storage Service (S3) – AKA a “Bucket”
Simple Storage Service (S3) – AKA a “Bucket”
Some Challenges for Our Profession
How Do You Audit a Function?
How Do You Audit an Algorithm?

Let \( a = bq + r \), then find a number \( u \) which divides both \( a \) and \( b \) (so that \( a = su \) and \( b = tu \)), then \( u \) also divides \( r \) since

\[
    r = a - bq = su - qt u = (s - qt) u.
\]

Similarly, find a number \( v \) which divides \( b \) and \( r \) (so that \( b = s' v \) and \( r = t' v \)), then \( v \) divides \( a \) since

\[
    a = bq + r = s' v q + t' v = (s' q + t') v.
\]

Therefore, every common divisor of \( a \) and \( b \) is a common divisor of \( b \) and \( r \), so the procedure can be iterated as follows:

\[
\begin{align*}
q_1 &= \left[ \frac{a}{b} \right] _1 \\
q_2 &= \left[ \frac{b}{r_1} \right] _1 \\
q_3 &= \left[ \frac{r_1}{r_2} \right] _1 \\
q_4 &= \left[ \frac{r_2}{r_3} \right] _1 \\
q_n &= \left[ \frac{r_{n-2}}{r_{n-1}} \right] _1 \\
q_{n+1} &= \left[ \frac{r_{n-1}}{r_n} \right] _1
\end{align*}
\]
How Do You Audit a Script?
Some Key Takeaways...

Cloud services, notably AWS, Azure & GCP, offer some powerful tools for auditing including:

- Inventory & Access Management Tools
- Resource Allocation, Budget Limits & Locations
- Tags

Cloud services are also distinct in many ways:

- Ephemeral resources & functions
- Change management at cloud scale
- Skills & competencies are different
Our organizations have great resources to facilitate cloud audits.
There are some great resources to further your understanding of this topic:


https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx

Preguntas y Quejas?
Thank you!

Matt Stamper
CISO | Executive Advisor
MPIA, MS, CISA, CISM, CIPP-US, ITIL
mstamper@evotek.com : 760-809-2164