AUDIT PROGRAM NARRATIVE

AMAZON WEB SERVICES® (AWS®) AUDIT PROGRAM

ISACA®

CONTENTS

ABSTRACT

While every Amazon Web Services® (AWS®) deployment may be tailored to suit the enterprise's unique needs, certain common considerations in areas such as network configuration, logical access controls, logging and event management, to name a few, apply to many enterprises. ISACA® addresses these and other topics in the *Amazon Web Services® (AWS®) Audit Program* to assist IT auditors as they assess AWS environments.

Amazon Web Services® (AWS®) Audit Program

Adoption of cloud services is projected to continue to increase such that by 2020, 41 percent of enterprise workloads will be hosted on public cloud platforms.[1] While there are other platforms, Amazon Web Services® (AWS®) is one of the front runners in the cloud services arena. Given its widespread use, IT auditors will benefit not only from understanding specifically how a given organization uses AWS services, but also from generally comprehending the operational, security and compliance elements of AWS. AWS developer and user guides are informative resources for IT auditors in creating an AWS audit universe and identifying specific risk areas to audit.

To assure that AWS services support operational and compliance objectives, ISACA's audit program considers AWS from diverse perspectives, across the following domains:

- Governance
- Network configuration and management
- Asset configuration and management
- Logical access control
- Data encryption control
- Security incident response
- Security logging and monitoring
- Disaster recovery

Audit Objectives

The objective of the audit program is to assist IT auditors in their assessments of AWS deployments. Accordingly, consideration is given to:

- Use of AWS services
- Access to the AWS environment
- Management and interrelationships of AWS services

Audit Scope

The audit program covers AWS applications and functions, as well as containers.

Business Impact and Risk

One of the most significant considerations in deploying AWS is its configuration. In the publication, "Top Ten Configuration Risks in AWS: Remediation Begins With Discovery," Palo Alto Networks® identified some of the default settings that may introduce risk to an enterprise's environment.[2] Examples of these settings—and the associated potential risk—include:

- **Administrative SSH login accessible from anywhere**. A breach here could result in a denial-of-service (DoS) attack and possible loss of data.
- **Single factor authentication**. With authentication limited to password (and no other factor), the password is the only credential needed for a malicious actor to gain access.
- **Identity and access management (IAM) groups and roles without access**. Lack of group/role access may result in more access granted to individuals, rather than to groups or roles, with the unintended outcome of more access than necessary being granted.

In addition to ensuring appropriate configuration during deployment, enterprises should consider agility. One of the primary reasons that enterprises adopt AWS is to implement change quickly. If the enterprise lacks AWS expertise (or access to AWS expertise), the level of agility it seeks may not be attained. Ultimately, this gap could result in a failure to align AWS services with strategic objectives.

[1] Columbus, Louis; "83 Percent of Enterprise Workloads Will Be In The Cloud by 2020," Forbes, 7 January 2018, https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#4ee9010d6261

[2] Palo Alto Networks®, "Top 10 Configuration Risks in AWS: Remediation Begins With Discovery," 2018, https://www.paloaltonetworks.com/resources/ebooks/top-10-aws-configuration-risks.html

Minimum Audit Skills

The *Amazon Web Services® (AWS®) Audit Program* assumes that auditors exercise due professional care and possess professional competencies culminating in the proficiency to conduct an audit. ITAF Standard 1005 and ITAF Guideline 2005 (Due Professional Care) require the auditor to exercise professional skepticism and maintain effective communication throughout the course of an audit. ITAF Standard 1006 and ITAF Guideline 2006 (Proficiency) require the auditor to have technical skill, knowledge and/or experience in the areas under assessment. This expectation is particularly relevant to auditors who do not hold the CISA or other appropriate designation.

Testing Steps

Refer to the accompanying spreadsheet file.

Acknowledgments

ISACA would like to recognize:

Lead Developer

Adam Kohnke
CISA, USA

Expert Reviewers

Robin Lyons
CISA, CIA, USA

Bhupinder Singh
CISA, CISM, USA

ISACA Board of Directors

Rob Clyde, Chair
CISM
Clyde Consulting LLC, USA

Brennan Baybeck, Vice-Chair
CISA, CRISC, CISM, CISSP
Oracle Corporation, USA

Tracey Dedrick
Former Chief Risk Officer with Hudson City Bancorp, USA

Leonard Ong
CISA, CRISC, CISM, CGEIT, COBIT 5 Implementer and Assessor, CFE, CIPM, CIPT, CISSP, CITBCM, CPP, CSSLP, GCFA, GCIA, GCIH, GSNA, ISSMP-ISSAP, PMP
Merck & Co., Inc., Singapore

R.V. Raghu
CISA, CRISC
Versatilist Consulting India Pvt. Ltd., India

Gabriela Reynaga
CISA, CRISC, COBIT 5 Foundation, GRCP
Holistics GRC, Mexico

Gregory Touhill
CISM, CISSP
Cyxtera Federal Group, USA

Ted Wolff
CISA
Vanguard, Inc., USA

Tichaona Zororo
CISA, CRISC, CISM, CGEIT, COBIT 5 Assessor, CIA, CRMA
EGIT | Enterprise Governance of IT (Pty) Ltd, South Africa

Theresa Grafenstine
ISACA Board Chair, 2017-2018
CISA, CRISC, CGEIT, CGAP, CGMA, CIA, CISSP, CPA
Deloitte & Touche LLP, USA

Chris K. Dimitriadis, Ph.D.
ISACA Board Chair, 2015-2017
CISA, CRISC, CISM
INTRALOT, Greece

About ISACA

Now in its 50th-anniversary year, ISACA® (isaca.org) is a global association helping individuals and enterprises achieve the positive potential of technology. Today's world is powered by information and technology, and ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations. ISACA leverages the expertise of its 460,000 engaged professionals—including its 140,000 members—in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology. ISACA has a presence in more than 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

DISCLAIMER

ISACA has designed and created the *Amazon Web Services® (AWS®) Audit Program* (the "Work") primarily as an educational resource for IT audit professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, IT audit professionals should apply their own professional judgments to the specific circumstances presented by the systems or information technology environment.

Reservation of Rights

ISACA®

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/aws-audit-program

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAHQ

Instagram:
www.instagram.com/isacanews/

Amazon Web Services® (AWS®) Audit Program
ISBN 978-1-60420-799-6