

# STOP CLOUD RISK: VERIFY YOUR AWS POSTURE AGAINST GLOBAL CIS STANDARDS

**Is Your Cloud Exposure Hidden?** Human error and configuration drift are the leading causes of data breaches in AWS. As an official **AWS Partner** and **CIS Member**, XTIVIA leverages proprietary CIS assessment tools to help you eliminate misconfigurations and establish a verified security baseline for your infrastructure. **For specialized services such as databases, we dynamically incorporate relevant, additional CIS Benchmarks to ensure full coverage of your unique environment.**

## Key Benefits: Secure Cloud Governance

- **Eliminate Human Error:** Identify and remediate "leaky" buckets and over-privileged roles before they lead to a breach.
- **Verified Expertise & Tools:** XTIVIA's status as an **AWS Partner** and **CIS Member**, combined with the use of official CIS assessment tools, guarantees your AWS posture is evaluated by certified professionals using the industry gold standard.
- **Fast-Track Compliance:** Achieve documented evidence of a hardened cloud posture to satisfy frameworks like SOC2, ISO 27001, and HIPAA.

## The XTIVIA 6-Point Cloud Security Audit

This assessment performs a comprehensive audit across the core pillars of your AWS environment:

- **Identity and Access Management (IAM):** Auditing root account usage, multi-factor authentication (MFA) requirements, password policies, the removal of unused credentials, and verification of the Principle of Least Privilege.
- **Logging and Monitoring:** Verifying that CloudTrail is enabled across all regions, integrated with CloudWatch Logs for real-time alerting on unauthorized API calls or policy changes, and ensuring CloudTrail logs are encrypted using AWS KMS.
- **Networking and Security Groups:** Evaluating VPC configurations, ensuring that security groups do not allow unrestricted ingress (0.0.0.0/0) to sensitive ports like SSH (22) or RDP (3389).
- **Storage and Encryption:** Checking for publicly accessible S3 buckets, enforcing Data-at-Rest encryption using AWS KMS for EBS volumes and RDS instances, and auditing account-level public access blocks for S3.
- **Compute and Configuration Security:** Auditing critical EC2 instance configurations, enforcing termination protection, and verifying use of protected metadata services (IMDSv2 adoption) to ensure secure compute controls.
- **Threat Detection & Automation:** Verifying that continuous security services like AWS GuardDuty and AWS Security Hub are enabled across all regions for proactive threat detection and compliance aggregation.

## READY TO SECURE YOUR CLOUD? Schedule a Free 15-Minute Consultation.

Cloud configuration drift is a constant risk. Don't wait for a breach—contact XTIVIA today for a confidential scoping call and gain full visibility into your cloud security and establish a verified baseline for your infrastructure.

Schedule your **AWS CIS Benchmark Assessment** today.

- **Email:** [info@xtivia.com](mailto:info@xtivia.com)
- **Website:** [www.virtual-dba.com](http://www.virtual-dba.com)
- **Call:** 888-685-3101, ext. 2
- **Learn More:** <https://virtual-dba.com/cis-security/>

## XTIVIA Overview

XTIVIA is a proven technology integration and innovation company known for delivering leading-edge technology solutions to our clients' specific requirements, regardless of project complexity. Since 1992, our success has stemmed from a demonstrated ability to deliver deep expertise via professional services, empowering clients to successfully, competitively, and profitably leverage their chosen technology. XTIVIA has offices in Colorado, New York, New Jersey, Texas, Virginia, and India. [www.xtivia.com](http://www.xtivia.com)