David O'Neal

MS, Cybersecurity · Certified GRC Engineer, Auditor Specialty (CGE-AUD) · ISO 27001 Lead Auditor (in progress)

(501) 749-4031 onealdavide@gmail.com linkedin.com/in/david-oneal github.com/doneal78 davidoneal.dev labs.davidoneal.dev

EXECUTIVE SUMMARY

Certified GRC Engineer, Auditor Specialty (CGE-AUD), with 8+ years in IT and security. That includes a SOC analyst role at Bank OZK, a bank that followed SOC 2, a state IT security role at the Arkansas Department of Public Safety, and MSSP work at Legato Security. Before security, I spent 11 years at Arkansas Children's Hospital, including biomedical equipment work. ISO 27001 Lead Auditor is in progress.

In my own AWS lab account I completed a ten-project compliance automation curriculum. The work includes a Terraform baseline, OPA/Rego policy tests, a GitHub Actions gate, Cosign-signed evidence, a SOC 2 evidence workbook built from Security Hub and Config, and an OSCAL system security plan for 21 NIST 800-53 controls. The lab account measured 40% AT RISK before controls, 78% NEEDS IMPROVEMENT after the Terraform baseline, and 83% GOOD after the ten projects.

PROJECTS

GRC Engineering Pipeline GitHub

Built an evidence-first CI/CD pipeline enforcing NIST 800-53 controls (SC-28, AC-3, CM-6, AU-3) on AWS S3 in my own lab account. Terraform defines the infrastructure. Six Rego policies via OPA/Conftest test the plan before deployment. GitHub Actions blocks non-compliant pull requests with branch protection. Cosign performs keyless signing of evidence artifacts with a Sigstore chain of custody. OSCAL 1.2.1 component definitions map every control to its evidence and validate with compliance-trestle.

Tools: Terraform, OPA/Rego, Conftest, GitHub Actions, Cosign, Sigstore, AWS (S3, CloudTrail, KMS, IAM) in my own lab account, Python, OSCAL, compliance-trestle

6/6 policy tests passing. A merged compliant pull request and a deliberately blocked regression pull request are in the commit history.

Compliance Automation Lab GitHub

Built an AWS S3 and IAM configuration scanner using Python and boto3 against a Terraform baseline in my own lab account, producing a before and after compliance score with root-cause detail on every failure.

Tools: Python, boto3, Terraform, AWS S3, AWS IAM, AWS Security Hub

Terraform baseline stage: 40% AT RISK to 78% NEEDS IMPROVEMENT in my own AWS lab account. The gap at 78% was one intentionally misconfigured test bucket and a physical MFA device pending setup on the lab IAM user, documented in the notes. After the ten projects, the same account measured 83% GOOD.

EXPERIENCE

Independent GRC Engineering

August 2026 to Present

Remote

- Independent GRC engineering work: completed a ten-project compliance automation curriculum in my own AWS lab account and earned CGE-AUD.
- Shipped an end-to-end compliance automation pipeline (Terraform, OPA/Rego, GitHub Actions, Cosign, OSCAL) mapped to NIST 800-53 controls SC-28, AC-3, CM-6, and AU-3, with 6 of 6 policy tests passing and a merged pull request plus a blocked pull request in the history.
- Project 11, an audit readiness pipeline from chapter 9 of the curriculum, is underway. The Certified GRC Engineer Practitioner course (CGE-P) is in progress. ISO 27001 Lead Auditor is in progress.

Project Manager

September 2025 to July 2026

Legato Security (Managed Security Service Provider)

- Led security service delivery for 10+ enterprise client accounts, coordinating across SOC analysts, engineers, and channel partners to keep projects on track.
- Built and managed onboarding workflows in GuideCX with milestone tracking that got new clients up and running faster.
- Wrote Quarterly Business Reviews (QBRs) and delivery updates translating technical security work into plain language for client leadership.
- Designed the connector setup workflow for Mave so engineers had a documented, repeatable process for configuring client integrations.

Rehired into this role after a company-wide reduction in force ended the Cybersecurity Consultant position below. Two months between roles.

Cybersecurity Consultant

April 2025 to July 2025

Legato Security

- Designed and led patch and vulnerability management programs for aerospace and industrial clients across 279+ endpoints, prioritizing CVEs by risk level and business impact.

- Used Tenable.io, Nessus, and PDQ Connect to cut critical vulnerability remediation from several weeks to under 72 hours, more than 80% faster.
- Built a Patching-as-a-Service delivery framework that standardized remediation across client environments and reduced manual coordination effort.
- Authored patching SOPs, risk classifications, and remediation documentation to strengthen governance and audit readiness.

State IT Security Specialist October 2024 to March 2025

Arkansas Department of Public Safety

- Maintained patch compliance above 95% across 500+ endpoints with PDQ Connect, through automated deployment and consistent remediation tracking.
- Handled IAM for the department, including provisioning, deprovisioning, MFA resets, and access reviews in Active Directory and Azure AD.
- Built vulnerability dashboards and KPI reports that gave IT leadership a clear picture of current risk.

Position eliminated due to state budget reallocation.

SOC Analyst October 2021 to June 2024

Bank OZK, a bank that followed SOC 2

- Investigated and resolved 30+ phishing, malware, BEC, and DLP incidents per week in a financial-sector SOC, completing phishing investigations in under 20 minutes while maintaining SLAs and documenting findings for audit.
- Reduced phishing false-positive alerts by 40% through detection rule tuning across Proofpoint, Microsoft Defender, and Cisco SEG.
- Wrote DLP response SOPs that standardized how the team handled incidents and kept everything traceable.
- Worked with the security awareness team on phishing simulations and reporting habits. Phishing incidents dropped 40% over the same period.

System Operations Analyst I June 2017 to October 2021

FIS Global

- Provided 24/7 enterprise systems monitoring using Splunk, and used PDQ Deploy for patch deployment, responding in real time to service disruptions and supporting incident root cause analysis.
- Maintained operational playbooks and documentation to support audit compliance and SLA consistency.
- Coordinated with global support teams.

SKILLS

Compliance Automation and Policy-as-Code

OPA/Rego, Conftest, Sigstore/Cosign, OSCAL 1.2.1, compliance-trestle, NIST 800-53, SOC 2

Infrastructure as Code

Terraform, GitHub Actions, AWS (S3, CloudTrail, KMS, IAM)

Compliance and Risk Management

Risk register management, remediation tracking, patch compliance tracking, KPI and dashboard reporting

Security Operations

SIEM tuning, phishing, malware, BEC, and DLP investigation, detection engineering, incident response

Identity and Access

Active Directory, Azure AD, MFA enforcement, provisioning and deprovisioning, access reviews

Vulnerability Management

Tenable.io, Nessus, PDQ Deploy, PDQ Connect, CVSS-based prioritization

Languages and Tools

Python, boto3, Bash, JSON, YAML

EDUCATION

Master of Science (MS), Cybersecurity
Maryville University

Bachelor of Science (BS), Information Technology
University of Arkansas Grantham

CERTIFICATIONS

Certified GRC Engineer, Auditor Specialty (CGE-AUD) GRC Engineering Club — 2026 · Verify

ISO 27001 Lead Auditor — In progress

GRC Jumpstart: GRC Foundations in Cybersecurity SimplyCyber — 2024

VMDR (Qualys): Vulnerability Management Detection and Response Qualys — 2024