JAMAL DAVISON

New York, NY | 646-444-7941 | JamalDavisonIT@outlook.com | linkedin.com/in/jamaldavison

INFORMATION SECURITY & GRC PROFESSIONAL | PCI DSS | IAM | IT CONTROLS

Information Security and GRC professional with 25+ years supporting regulated industries and military operations.
Expertise in PCI DSS, HIPAA, ISO 27001, SOC 2, NIST CSF, IAM, IT controls, and audit readiness.
Resolved audit findings, cut access-governance errors 30%, and improved operations through automation.

SUMMARY OF ACCOMPLISHMENTS

- Designed and operated IT General Controls across access management, change control, and computer operations, supporting nine consecutive successful annual PCI DSS assessments spanning v3.2.1 through v4.0.1.
- Resolved all seven PCI DSS findings identified across the final three assessments, achieving zero outstanding findings.
- Reduced access-governance errors by approximately 30% and saved three to five hours of manual effort weekly by standardizing operations through nearly 50 authored SOPs and PowerShell automation integrated with Jira and Confluence.
- Supported identity-lifecycle operations as part of a team serving 5,000+ users across Active Directory, Microsoft Entra ID, Okta, and Microsoft 365 in a regulated healthcare environment.

AREAS OF EXPERTISE

- **Compliance Frameworks:** PCI DSS v4.0.1 • HIPAA • ISO 27001 • SOC 2 • NIST CSF 2.0 • DoD Information Assurance
- **Security Program Management:** Information Security & GRC Programs • IT General Controls • Risk Assessments • Audit Readiness • Compliance Documentation • Policy Development • Control Design • Change Management • Configuration Management
- **Identity & Infrastructure:** Identity & Access Management • Active Directory • Microsoft Entra ID • Okta • Microsoft 365 • Microsoft Azure • AWS • Network Security • Infrastructure Security • Cryptographic Key Management
- **Monitoring & Response:** SIEM & Security Monitoring • Rapid7 InsightIDR • Vulnerability Remediation • Risk Prioritization • Log Analysis • Alert Triage • Threat Detection • Incident Response • Security Investigations

PROFESSIONAL EXPERIENCE

Intechgrity Solutions, New York, NY **July 2021 - Present**
Cybersecurity & Infrastructure Consultant
Contract engagement, ongoing since 2021; ran concurrently with full-time role at Affinity Solutions through October 2025.

- Supported identity-lifecycle operations as part of a team serving 5,000+ users across Active Directory, Microsoft Entra ID, Okta, and Microsoft 365, including onboarding, role changes, and terminations within a regulated healthcare environment.
- Maintained validated external backups under a documented 180-day retention policy, performed and documented weekly restore testing, and completed frequent mailbox-item recoveries to support business continuity and data restoration.
- Restored 20 of 25 corrupted virtual machines during a major security event, minimizing downtime and supporting business continuity.
- Led 12 technicians in migrating 500 of 1,000 trading-floor turrets from legacy to IP-based infrastructure for Tier-1 financial institutions, including JPMorgan Chase, Bank of America, Goldman Sachs, Citigroup, and Nomura.
- Led secure-communications validation across 500 migrated turrets and call-recording testing on approximately 250 recording-enabled units.

Affinity Solutions, New York, NY **January 2015 - October 2025**

Desktop Support Technician | GRC & Security Operations Analyst

- Reduced access-governance errors by approximately 30% and saved three to five hours of manual effort weekly by authoring nearly 50 SOPs covering provisioning, terminations, access reviews, patching, and incident response, then automating repeatable processes with PowerShell, Jira, and Confluence.
- Conducted quarterly access reviews that identified 10-15 accounts requiring remediation per cycle, helped remediate three major enterprise access-control weaknesses, and enforced MFA-protected access across 450+ endpoints while coordinating timely deprovisioning and least-privilege access with HR.
- Reviewed vulnerability findings imported into Rapid7 InsightIDR across 450+ endpoints, coordinating approximately 90% of critical and high-risk remediation within risk-based SLAs and PCI DSS patching timeframes and personally deploying same-day fixes for zero-day and out-of-band patches.
- Supported PCI DSS compliance activities and evidence across all 12 requirements and SOC 2 controls covering change management, availability monitoring, access governance, incident response, and email DLP designed to prevent PII exfiltration.
- Managed Microsoft Entra ID permissions and AWS S3 storage under least-privilege principles, hardened Linux and Windows servers, demonstrated firewall and network configurations to auditors, and supported Cisco VPN migration, physical-access controls, and secure drive destruction within the cardholder data environment.
- Led incident-response investigations that reduced ticket volume by approximately 25% and separately reduced user downtime by approximately 25%, partnering with IT, HR, Compliance, and executive leadership to accelerate evidence collection and translate regulatory requirements into business terms.

New York eHealth Collaborative, New York, NY **February 2012 - June 2014**

Lead Service Desk Analyst | Change & Access Governance

- Designed and established a five-person Change Approval Board with standardized ticket requirements and risk-assessment checkpoints, reducing recurring outages and failed changes while improving availability from 99.8% to 99.9% and reducing potential annual downtime by approximately 50%.
- Reviewed approximately 12 security alerts weekly for potential unauthorized-access and credential-sharing activity, supporting root-cause analysis and HIPAA-aligned controls protecting electronic protected health information.
- Supported a team responsible for access controls and security oversight across five RHIO platforms.
- Authored SOPs and compliance documentation aligning operational workflows with regulatory requirements and internal control standards.

Citigroup, New York, NY **January 2010 - February 2012**

System Administrator | IT Asset & Endpoint Security

- Implemented IT asset-governance controls, barcode-based tracking, and recurring audits across 1,000+ computers, printers, and thin clients, improving inventory accuracy by 10 percentage points, from 80% to 90%.
- Built centralized technical documentation and equipment databases covering 250+ combined printers and thin clients with one additional technician.
- Maintained endpoint-security controls, conducted vulnerability assessments, and remediated identified risks.

Macmillan, New York, NY **June 2004 - January 2009**

System Administrator | IT Operations & Incident Response

- Supported 1,200+ users across four sites as part of the systems-administration and technical-support team, managing a shared queue averaging approximately 100 daily tickets against tiered response and resolution SLAs ranging from one to seven hours.
- Served as the on-call incident-response lead one week per month, meeting severity-based callback SLAs of 30-60 minutes and supporting traveling sales representatives nationwide.
- Developed and implemented security policies and risk assessments aligned with ITIL v2, reducing legal and financial exposure.

United States Air Force, Global Locations **November 1999 - November 2003**

Deployable Network Administrator | Network Security

- Reduced military network-deployment time by approximately 25% through standardized configurations and network segmentation.
- Configured and secured SIPRNet connectivity in accordance with applicable DoD information-assurance and COMSEC requirements.

- Supported 24 military missions, exercises, and COMSEC inspections across global locations without a known security incident, passing all formal inspections without compliance findings.
- Managed cryptographic-key handling, storage, accountability, and destruction to protect classified information.

EDUCATION

Master of Science - Network & Communications Management
DeVry University, 2017
Bachelor of Science - Network & Communications Management
DeVry University, 2013

CERTIFICATIONS & PROFESSIONAL DEVELOPMENT

- ISO/IEC 27001:2022 Lead Auditor - Mastermind (June 2025)
- NIST Cybersecurity Framework 2.0: Managing Risks - Packt/Coursera (July 2026)
- Microsoft Cybersecurity Analyst Professional Certificate - Microsoft/Coursera (June 2026)
- Google Cybersecurity Professional Certificate - Coursera (June 2026)
- Google Project Management Professional Certificate - Coursera (June 2026)
- AI Security & Governance - Securiti (November 2025)
- Lean Six Sigma Green Belt - Star Global College of Workforce Development (December 2025)
- Vulnerability Management - Qualys (June 2021)