GalaLayo

Capabilities Statement

Founded in 2019, GalaLayo helps organizations across the United Sates stay ahead of evolving cyber threats with practical, forward-looking security solutions. We simplify complex risk environments, strengthen enterprise defenses, and align cybersecurity with mission and business goals Our focus is clear: reduce risk, improve operational resilience, and deliver measurable security outcomes that support performance and long-term value.

Core Competencies

- **Risk Assessment & Governance**
  - Enterprise risk assessments aligned to NIST CSF and RMF methodology
  - System security categorization (FIPS 199) and impact analysis
  - Gap analysis for FedRAMP, FISMA High, and CMMC compliance
  - Policy development and governance program maturation
  - Continuous risk scoring and executive reporting dashboards
- **Vulnerability Assessment & Penetration Testing (VAPT)**
  - Network, cloud, web application, API, mobile, and wireless testing
  - Manual and automated assessments aligned with OWASP and NIST standards
  - FedRAMP-ready security testing and control validation
  - Adversarial simulation to evaluate Zero Trust control effectiveness
- **Threat Intelligence & Continuous Monitoring**
  - AI-driven threat detection and behavioral analytics
  - Identity Threat Detection & Response (ITDR)
  - Security Information & Event Management (SIEM) integration
- **Managed Cybersecurity & Zero Trust Enablement**
  - Zero Trust maturity assessments and roadmap development
  - Micro-segmentation, ZTNA, and continuous authentication
  - Risk- and context-aware access enforcement
  - Automated compliance validation and audit readiness
  - Managed security operations supporting FedRAMP and CMMC environments
- **Incident Response & Recovery**
  - Incident containment, eradication, and forensic analysis
  - Regulatory breach impact assessment and reporting support
  - Playbook development aligned to federal IR control families
  - Post-incident control validation and security posture improvement
  - Recovery planning and resilience testing
  - Micro-segmentation, ZTNA, and continuous authentication
  - Risk- and context-aware access enforcement
  - Managed security operations supporting FedRAMP and CMMC environments

NAICS and PSC Codes

- **NAICS:**
  - 541512 – Computer Systems Design Services
  - 541519 – Other Computer Related Services
  - 541611 – Admin Mgmt. and General Mgmt. Services
  - 541690 – Other Scientific and Technical Services
  - 541990 – All Other Professional & Tech Services
- **PSC:**

D301, D302, D306, D307, D308, D310, D311, D314, D316, D318, D319

Partners

PONDURANCE

Rizkly

G Ventures

eCi Consultants Inc.

HUNTRIX Professional Pentesting Services

bugcrowd

Past Performance

Extensive federal cybersecurity experience from his role at Delviom, where he supported DHS, FEMA, and GSA programs by delivering vulnerability assessments, penetration testing, RMF implementation, and compliance documentation aligned with NIST SP 800-53 and DHS 4300A standards. He has conducted penetration testing and vulnerability analysis for organizations including Zephon, Framework Security, and Desktop Alert's military-grade Ping Alert platform, supporting clients such as NATO, DoD, FEMA, and other regulated industries. His work spans secure software development oversight, cloud and web application testing, API and mobile assessments, supply chain risk initiatives, and governance efforts.

Corporate Information

- **CAGE:** 9YNMO **UEI:** L8FJUPC4ZJU3
- **Business POC:** Dwight Grupp
- **Phone:** (703) 463-8418
- **E-Mail:** dwight@galalayo.com
- **Address:** 8401 Mayland Dr, Ste S, Richmond, VA 23294
- **Work Area:** Nationwide