

# Mark Graziano

Security & GRC Leader, Host of The GRC Podcast

703.409.9942

mark.graziano.13@gmail.com



---

## Professional summary

Experienced Security & GRC leader and community voice with over a decade of expertise in cultivating cross-functional security champions and fostering proactive Security cultures. Committed to driving business growth and innovation through risk management and streamlined processes, aligned with organizational goals. Adept communicator skilled in promoting collaboration and accountability across diverse teams.

## Employment history

### Twilio Segment | Manager of Governance, Risk and Compliance | Nashville, TN

*Jul, 2021 - Present*

- Drive Security & GRC process enhancements through automation, optimizing scalability and reducing high-effort tasks.
- Lead customer calls with security stakeholders, securing over \$8M in ARR to date as the decisive factor.
- Implemented scalable automations to replace Segment's GRC tool, saving \$72K annually.
- Developed and managed SOC 2 Type 2 and ISO 27001/27018/27018 programs, impacting over \$135M in ARR.
- Led cross-functional efforts to develop Twilio's GDPR and CCPA compliance framework, ensuring data protection.
- Transformed data governance with AI-powered apps, enhancing policy UX and enforcement mechanisms.
- Drove the adoption and implementation of a modern Security/Privacy Trust Center (Safebase) across the entire enterprise.

### The GRC Podcast | Host

*May, 2023 - Present*

- Led the end-to-end creation and continued production of The GRC Podcast
- Challenging industry stereotypes and conventional wisdom by collaborating with security experts to offer practical career and program strategies

### Aptible | Data Protection Advisor | Nashville, TN

*Jan, 2021 - May, 2021*

- Directed risk management and compliance programs. Developed security policies and procedures and led compliance initiatives such as SOC 2, ISO, and HITRUST.
- Created and delivered security training. Guided executive leadership team and stakeholders in best practices for effective risk mitigation and security enablement.
- Identified and assessed potential data protection risks and vulnerabilities within the organization's operations and systems.

### NCC Group | Principal Security Consultant | Nashville, TN

*Oct, 2018 - Jan, 2021*

- Directed strategic Information Security initiatives, driving compliance with industry standards and government regulations. Led rigorous audits, risk analyses, and optimized security controls, focusing on FedRAMP, DFAR, ITAR, NIST CSF, CMMC, and PCI DSS.

- Managed a team of nine in Federal Services consulting, driving project ARR to \$3M, marking a 50% YoY surge. Formulated security policies, executed marketing campaigns, and fostered a GRC-supportive environment.
- Conducted comprehensive cybersecurity assessments on key sectors such as government facilities, food and agriculture, and financial services. Delivered gap assessments, compliance reports, and advised on PCI architecture.
- Enhanced the NCC Group ScoutSuite, a Python-based multi-cloud security auditing tool, bolstering development and maintenance efficiency.

## **Coalfire Systems | IT Security Consultant/Associate Security Consultant | Nashville, TN**

*Feb, 2015 - Oct, 2018*

Served as the VRM authority guiding executive leadership in initiatives to control costs, mitigate risks, and improve service. Served as the principal PCI DSS advisor for critical accounts. Led NSIT framework-based cyber risk assessments, delivering actionable insights to C-suite and Board. Curated strategic remediation roadmaps aligned with executive goals. Negotiated client fines with merchant banks, saving tens of thousands monthly. Instrumental in shaping the user experience (internal and external customers) of CoalfireONE, Coalfire's flagship compliance automation tool.

## **Booz Allen Hamilton | Associate Cybersecurity Consultant | Washington, DC**

*Feb, 2014 - Feb, 2015*

Delivered impactful information security initiatives for high-stake government projects. For the Pentagon, led a comprehensive risk assessment, paving the way for a successful transition from DIACAP to the Risk Management Framework. In a separate engagement with the U.S. Air Force, provided essential Certification and Accreditation support, resulting in multiple system accreditations and an Authorization to Operate, and bolstered security through rigorous SCAP and STIG testing. Concurrently, assessed security protocols at EPA-managed water treatment plants in Virginia, ensuring stringent standards were met.

## **Teklogic | Network Engineer I | Chesapeake, VA**

*May, 2013 - Feb, 2014*

Specialized in enhancing network security, optimizing performance, and managing virtualized environments. Through collaborative risk assessment, I've contributed to network resilience and operational excellence.

# **Education**

**Christopher Newport University, Newport News, VA | Bachelor of Science (B.S.), Computer Engineering**

# **Skills**

GRC Solutions & Automation  
Risk Management & Mitigation  
AI Governance  
GRC Roadmap Development  
Security Awareness Training  
Policy Creation & Management

People Management  
Audit Preparation & Management  
Contract Review  
Data & Cloud Security  
Information Security Marketing  
ISO, SOC2, HITRUST, FedRAMP, DFARS, DIACAP, ITAR, NIST RMF/CSF, CMMC, PCI DSS, HIPAA

# **Links**

[The GRC Podcast](#)

[LinkedIn Profile](#)