Christophe Foulon

760-880-5395 - christophefoulon@gmail.com - linkedin.com/in/christophefoulon

EDUCATION

Master of Science, Information Technology - Information Assurance/Cybersecurity - Walden University

Bachelor of Science, Business Administration - Information Systems – Walden University

CERTIFICATIONS & Clearances

Active: ISC2 – **CISSP | SANS** – **GSLC**

Expired: ISACA - **CRISC**, **CDPSE | AWS Certified Security - Specialty**, **Cloud Practitioner |** CompTIA **A+**, CompTIA **Network+,** CompTIA **Security+ z |** Microsoft Server 2003 **MCSA**, **MCSA Sec**, **MCSE |** Previous TS Clearance

Objective: *Chief Information Security Officer (CISO) executive leadership role*

Chief Information Security Officer executive leadership role

My expertise lies in developing and executing organizational-wide cybersecurity strategies that align with business goals, mitigate risks, ensure regulatory compliance, and enable technological innovation and growth.

Strategic Cybersecurity Leadership: Successfully transformed the cybersecurity landscape of a Fortune 10 Fintech company, responding to an active exploit by implementing a multi-layered security strategy.

Digital Transformation and Cloud Security: Led a comprehensive digital transformation for a federal agency, seamlessly integrating cloud migration with enhanced cybersecurity and operational maturity. This involved meticulous planning, execution, and management of the transition to AWS Cloud, ensuring agility and security in the agency's technological infrastructure.

Cybersecurity Portfolio Management: Demonstrated a keen insight in cybersecurity portfolio management, overseeing a significant growth of $10M in projects over five years. This included expanding the Azure Cloud Operations Site Reliability Engineering team by 50% and establishing robust 24/7 incident and issue management protocols.

Areas of Expertise

Digital Transformation & Cloud Security Integration | Operations Management in Diverse Technological Landscapes | Comprehensive Risk Assessment & Mitigation Strategies | Developed Governance Regulatory Compliance Programs | Incident Response Coordination and Disaster Recovery Planning | Development of Talent Pipelines and Strategic Relationships | Cross-functional team Leadership with a Consultative Approach | Development and Implementation of Security Policies and Procedures | Architecture & Solution Design and Delivery in Azure & AWS Cloud Environments | Program Management Across Healthcare, Finance, and Government | Executive and Board Briefings | Budget Management

WORK EXPERIENCE

CPF COACHING LLC – A CYBERSECURITY FOCUSED COACH/CONSULTANT **2007 - PRESENT**

CPF Coaching LLC specializes in offering fractional Virtual Chief Information Security Officer (vCISO) services, providing businesses with expert cybersecurity leadership flexibly. This unique approach allows organizations to benefit from top-tier security expertise without needing a full-time executive position, effectively managing cyber risks and aligning security strategies with business objectives.

Beyond cybersecurity, CPF Coaching LLC extends its services to comprehensive risk assessments and executive leadership/business coaching, empowering organizations to identify vulnerabilities, mitigate risks, and foster a

culture of resilience. Their holistic approach addresses technical security challenges and enhances leadership capabilities and strategic vision, driving business growth and operational excellence.

Subcontracted roles include:

Fractional CISO at Nexigen

Fractional Cybersecurity Engineer on the vCISO Team at SideChannel

CAPITAL ONE, MCLEAN, VA **OCTOBER 2020 - OCTOBER 2023**

SENIOR MANAGER, CYBERSECURITY & TECHNOLOGY RISK OVERSIGHT

In a pivotal role at the intersection of technology and business, led the strategic oversight of cybersecurity and technology risk across diverse lines of business (LOB). Championed the development and implementation of a comprehensive cybersecurity framework, aligning with organizational objectives and enhancing the security posture of Capital One.

Strategic Leadership in Cybersecurity: Directed a team of cybersecurity professionals and technology risk managers, fostering a security awareness and resilience culture. I have implemented innovative cybersecurity strategies and practices to protect organizational assets and data across multiple platforms, including AWS Cloud.

Risk Management and Compliance: Played a crucial role in identifying, evaluating, and mitigating cybersecurity risks, ensuring alignment with regulatory requirements and industry best practices. Developed and maintained a robust technology risk framework, significantly enhancing the organization's risk intelligence and response capabilities.

Incident Response and Vulnerability Management: Led the rapid response to an active exploit vulnerability, orchestrating a cross-functional team to mitigate the threat efficiently. We have implemented a proactive approach to vulnerability management, reducing the attack surface and enhancing system resilience.

Technology Risk Program Enhancement: Elevated the effectiveness of technology risk programs by challenging and improving existing processes, controls, and capabilities, focused on critical areas such as application resiliency, site reliability engineering (SRE), and change/asset management.

Cybersecurity Metrics and Reporting: Advanced the organization's cybersecurity and vulnerability management and risk management metrics maturity, collaborated on developing customized dashboards and data-driven reports for senior executives and stakeholders.

Project Leadership and Stakeholder Engagement: Managed the high-visibility Top of House US Card Project, strategically delegating critical tasks and ensuring comprehensive plans of action to address evolving security threats.

Threat Intelligence & Threat Profiling: *Developed bi-annual LOB Threat Profile reports*, providing key stakeholders with a clear understanding of the cybersecurity landscape and enabling targeted risk management strategies.

This custom TI Report focuses on strategic leadership, risk management, and effective stakeholder communication. It significantly contributes to Capital One's robust cybersecurity framework and enhances the organization's overall security culture. I drove threat profiling campaigns with internal business applications.

GRIMM SMFS INC, WASHINGTON D.C **DECEMBER 2019 – OCTOBER 2020**

SENIOR SECURITY CONSULTANT (SMF)

I led the provision of sophisticated cybersecurity and risk advisory services to federal and commercial clients, addressing their complex security challenges. My approach was to resolve immediate issues and foster a long-term, strategic vision of cybersecurity aligned with business objectives.

Strategic Cybersecurity Leadership: Guided executives and security leaders in understanding and addressing the broader impact of cybersecurity risks on their operations. I have leveraged my expertise to align cybersecurity strategies with business goals, ensuring a resilient and adaptive security posture.

Advanced Risk Assessment and Mitigation: Developed and conducted workshops and tabletop exercises tailored to client needs. These sessions were instrumental in evaluating cybersecurity risks, developing response strategies, and enhancing the overall risk awareness among key stakeholders.

Innovative Solutions for Cybersecurity Challenges: Spearheaded the design and implementation of customized, comprehensive Governance, Risk, and Compliance (GRC) programs, incorporating frameworks such as NIST CSF, CMMC, and ISO27001. This approach significantly improved clients' cybersecurity maturity and compliance posture.

Cybersecurity Program Development: I played a pivotal role in creating a cyber maturity builder program incorporating six adversarial and three defensive modules. This program enhanced clients' defensive capabilities and preparedness against sophisticated cyber threats.

Operational Risk Management: Delivered critical business impact reports and conducted thorough risk, cybersecurity program, and threat model assessments. My insights and recommendations were crucial for mitigating operational risks and strengthening cybersecurity defenses.

Cyber Range Training Platform Development: Led the development of an innovative cyber range training platform. This initiative provided clients hands-on experience tackling real-world cybersecurity scenarios, significantly enhancing their detection and response capabilities.

CONQUEST FEDERAL, WASHINGTON D.C **FEBRUARY 2019 – December 2019**

LEAD CYBER RISK MANAGEMENT CONSULTANT

In this leadership role at a federal consulting startup, I was pivotal in shaping and executing a comprehensive cybersecurity strategy focusing on cloud security, risk management, and organizational transformation. We managed a diverse team of 15 professionals, from analysts to senior project managers, focusing on developing their skills and aligning their efforts with strategic objectives.

Strategic Cybersecurity Leadership: Oversaw the delivery of critical risk, security, and cloud security consulting services with a $5M project budget. My strategic vision and direction were instrumental in guiding a federal agency through a significant digital transformation, enhancing cybersecurity maturity, and fostering cloud adoption.

Cloud Security and Digital Transformation Expertise: Played a crucial role in advising and assisting the federal agency with their migration to cloud services, including Microsoft Office365 & Azure Gov. Implemented advanced security and identity management technologies from Microsoft EMS, ensuring a seamless and secure transition to cloud environments.

Governance and Policy Development: Develop and implement robust governance frameworks, policies, and procedures tailored to enhance Federal Information Security Management Act (FISMA) compliance levels. This initiative led to a more structured and risk-aware cybersecurity posture within the agency.

Risk-Based Cybersecurity Management: Championed a risk-based approach to vulnerability management, significantly improving the agency's security posture and readiness. My leadership in this area was crucial in preparing the agency to adopt managed security services and manage third-party vendor risk profiles effectively.

Enhancing Cybersecurity Maturity: Provided strategic insights and guidance for the effective detection, response, and recovery mechanisms, contributing significantly to the maturation of the agency's organizational defenses. This included preparing for the onboarding of security service providers and managing the overall cybersecurity lifecycle.

Operational Cybersecurity Excellence: Through my leadership, the agency saw a marked improvement in FISMA maturity levels. The agency's cybersecurity operations were significantly enhanced by instituting a proactive and risk-informed approach, establishing a robust foundation for ongoing security management and compliance.

In this role, my focus was not just on addressing immediate cybersecurity challenges but on driving long-term, strategic change in cybersecurity practices, positioning the agency for a secure and innovative future.

Christophe Foulon
760-880-5395 - christophefoulon@gmail.com - linkedin.com/in/christophefoulon

AVANADE/ACCENTURE, RESTON, VA **AUGUST 2017 – FEBRUARY 2019**
MANAGER INFORMATION SECURITY CONSULTING

Led Microsoft Azure Fed Cloud Team, directed Managed Services to onboard/train new Gov Cloud Ops support members. I coordinated with legacy vendor support for project growth solutions and optimized the Ops SRE team for 24/7 incident/problem management across multiple locations. I drove program/project management for ten-million-dollar programs and managed finances/resources/strategic planning. Assessed Ops/Security/Compliance processes in FEDRAMP, identified vulnerabilities, and provided mitigating/remediation measures.

- It facilitated $10M project growth over five years, increasing the Microsoft Azure Government Cloud Operations Site Reliability Engineering team by 50% while providing 24/7 incident and issue management.
- Achieved 100% FEDRAMP compliance of new services, facilitated an audit process to ensure and adhere to FEDRAMP standards, shaped operation assessments, and provided risk mitigation to security and compliance vulnerabilities.

CANCER TREATMENT CENTERS OF AMERICA (CTCA), BOCA RATON, FL **SEPTEMBER 2014 – AUGUST 2017**
IS SITE SUPERVISOR

As the information security specialist, I shaped training and education for corporate users on cybersecurity, PHI, and PII. I have integrated security awareness into daily activities to promote a culture of security. Consulted on information security, assurance, and risk management during new project creativity and development with business units. Enforced security hardening policies and procedures for computers and mobile devices. I participated in an ad-hoc Information Security Team to manage and respond to security threats and incidents, including virus and malware remediation.

Supported risk reduction of major third-party related vendors, identifying and initiating information technology and security-related projects to ensure sensitive information complied with HIPAA.

ENTREPRENEURIAL ENDEAVOR

CPF COACHING LLC **JANUARY 2007 – PRESENT**

Engage with clients to provide cybersecurity and risk advisory solutions to their complex cybersecurity challenges. Founded and cohosted the "Breaking into Cybersecurity" Podcast; Principal Coach at CPF-Coaching.com.

- Authored Mastering LLMs and other courses for customized learning and development efforts.
- Authored "Developing Your Cybersecurity Career Path" , 'Hack the Cybersecurity Interview" and contributed to "Understanding and Measuring Cyber Risk" by Ryan Leirvik.

BOARD MEMBERSHIPS & AFFILIATIONS

INFRAGARD **2016 – Present**

InfraGard NCR - **IT Co-Sector Chief** (2018- 2023), **President** (2023 – Present)
InfraGard NCR – Member (2017- Present)

ISSA / ISACA / ISC2 – Regional Chapters **2017 - Present**

CISO & EXECUTIVE BOARD MEMBER - WORKFORCE RESEARCH & DEVELOPMENT **Jan 2021 – Present**
Whole Cyber Human Initiative