Christophe Foulon
760-880-5395 - christophefoulon@gmail.com - LinkedIn

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

Chief Information Security Officer

My Information Security expertise encompasses developing and executing comprehensive, organization-wide cybersecurity strategies that align with business goals, mitigate risks, ensure regulatory compliance, and foster technological innovation and growth. I have successfully transformed the cybersecurity landscape at a Fortune 10 Fintech company, responding to active exploits with a robust multi-layered security strategy.

In my leadership role, I spearheaded a digital transformation for a federal agency, integrating cloud migration with enhanced cybersecurity measures and operational maturity. This involved meticulous planning and execution and managing the transition to AWS Cloud to ensure agility and security in the agency's technological infrastructure.

Additionally, I have a strong track record in cybersecurity portfolio management, overseeing significant growth with an increase of $10M in projects over five years. My efforts included expanding the Azure Cloud Operations Site Reliability Engineering team by 50% and establishing robust 24/7 incident and issue management protocols, demonstrating deep insights and effective management in evolving cybersecurity environments.

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 **2007 – PRESENT**
CYBERSECURITY ADVISOR/FOUNDER

CPF Coaching LLC is a security consulting company focused on SMBs from 1-500 people

CPF Coaching LLC specializes in providing fractional Virtual Chief Information Security Officer (vCISO) services, offering businesses flexible, expert cybersecurity leadership. This innovative service model allows organizations to access top-tier security expertise without the commitment to a full-time executive, enhancing their ability to manage cyber risks and align security strategies with business objectives. CPF Coaching also extends its offerings to include comprehensive risk assessments and executive leadership/business coaching, empowering organizations to identify vulnerabilities, mitigate risks, and cultivate a culture of resilience. This holistic approach

not only addresses technical security challenges but also boosts leadership capabilities and strategic vision, fostering business growth and operational excellence. I have supported companies like MSSPs as a Fractional CISO at Nexigen & Format Cyber, a Fractional Cybersecurity Engineer on the vCISO Team at SideChannel, and executive cybersecurity consulting for start-up healthcare companies and franchisees.

CAPITAL ONE, MCLEAN, VA **OCTOBER 2020 - OCTOBER 2023**
SENIOR MANAGER, CYBERSECURITY & TECHNOLOGY RISK OVERSIGHT

Capital One Financial Corp. is a $50+ million retail credit company with 50,000+ stakeholders..
In a pivotal role at the intersection of technology and business, I led the strategic oversight of cybersecurity and technology risk across various lines of business at Capital One. I championed developing and implementing a comprehensive cybersecurity framework, aligning it with organizational objectives to enhance the overall security posture. I directed a team of cybersecurity professionals and technology risk managers, fostering a security awareness and resilience culture. My leadership included implementing innovative cybersecurity strategies and practices to protect organizational assets and data across multiple platforms, including AWS Cloud, significantly bolstering our defense mechanisms against emerging threats.

- **Risk Management and Compliance:** Identified, evaluated, and mitigated cybersecurity risks, aligning with regulatory requirements and best practices; developed and maintained a robust technology risk framework, enhancing organizational risk intelligence and response capabilities.
- **Incident Response and Vulnerability Management:** Led rapid response to active exploit vulnerabilities, orchestrating a cross-functional team for efficient threat mitigation; implemented proactive vulnerability management strategies to reduce attack surfaces and enhance system resilience.
- **Technology Risk Program Enhancement:** Improved the effectiveness of technology risk programs by enhancing processes, controls, and capabilities in critical areas like application resiliency, site reliability engineering (SRE), and change/asset management.
- **Cybersecurity Metrics and Reporting**: Advanced the maturity of cybersecurity metrics, vulnerability, and risk management; developed customized dashboards and reports for senior executives and stakeholders.
- **Project Leadership and Leadership Engagement**: Managed the high-visibility Top of House US Card Project, strategically delegating tasks and ensuring action plans to address security threats.
- **Threat Intelligence & Threat Profiling**: Produced bi-annual Line of Business (LOB) Threat Profile reports, enhancing stakeholder understanding of the external cybersecurity landscape, internal risk concerns, and vendor supply chain risks and enabling targeted risk management strategies. I led threat profiling campaigns for internal business applications, contributing significantly to a robust cybersecurity framework.

GRIMM SMFS INC, WASHINGTON D.C **DECEMBER 2019 – OCTOBER 2020**
SENIOR SECURITY CONSULTANT (SMF)

Grimm SMFS INC is a boutique security consulting company focused on solving its customers' complex problems
I spearheaded sophisticated cybersecurity and risk advisory services for federal and commercial clients, adeptly handling complex security challenges. My dual-focused approach resolved immediate issues and fostered a long-term, strategic cybersecurity vision aligned with business objectives. I guided executives and security leaders to comprehend and address the broader impacts of cybersecurity risks on their operations. Leveraging my expertise, I aligned cybersecurity strategies with business goals, ensuring a resilient and adaptive security posture for sustained organizational success.

- **Advanced Risk Assessment and Mitigation:** Developed and led client-specific workshops and tabletop exercises, enhancing cybersecurity risk awareness and response strategies among stakeholders.

- **Innovative Cybersecurity Solutions:** Spearheaded the creation of customized Governance, Risk, and Compliance (GRC) programs integrating frameworks like NIST CSF, CMMC, and ISO27001, improving clients' cybersecurity maturity and compliance.
- **Cybersecurity Program Development:** Created a cyber maturity builder program with six adversarial and three defensive modules, boosting clients' defense capabilities and preparedness against advanced cyber threats.
- **Operational Risk Management:** Produced critical business impact reports and conducted comprehensive assessments of risks, cybersecurity programs, and threat models, providing key insights for operational risk mitigation and cybersecurity enhancement.
- **Cyber Range Training Platform Development:** Led the development of a cyber range training platform, providing clients with practical experience in real-world cybersecurity scenarios, significantly improving their detection and response skills.

While working with a red teamer, I developed blue team visibility approaches by developing proof-of-concept dashboarding capabilities with the client's log management solution, using the MITRE ATT&CK framework and the tactics, techniques, and procedures (TTPs) that advance persistent threat (APTs) actors in their sectors.

CONQUEST FEDERAL, WASHINGTON D.C **FEBRUARY 2019 – December 2019**
LEAD CYBER RISK MANAGEMENT CONSULTANT

Conquest Federal is a federally focused security consultancy and MSSP
In a critical leadership role, I developed and implemented a comprehensive cybersecurity strategy, focusing on cloud security, risk management, and organizational transformation. I managed and mentored a diverse team of 15 professionals, from analysts to senior project managers, enhancing their skills and aligning their efforts with strategic objectives. I also oversaw the delivery of critical risk, security, and cloud security consulting services, managing a $5M project budget. My strategic vision and leadership were pivotal in guiding a federal agency through an extensive digital transformation, significantly improving cybersecurity maturity, and advancing cloud adoption.

- **Cloud Security and Digital Transformation Expertise**: Advised on federal agency's migration to cloud services, including Microsoft Office365 & Azure Gov; implemented Microsoft EMS security and identity management technologies, ensuring secure cloud transition.
- **Governance and Policy Development**: Developed and implemented governance frameworks and policies enhancing FISMA compliance; structured and risk-aware cybersecurity posture initiatives within the agency.
- **Risk-Based Cybersecurity Management**: Led a risk-based vulnerability management approach, enhancing the agency's security posture and readiness; prepared the agency for managed security services and effective third-party vendor risk management.
- **Enhancing Cybersecurity Maturity**: Delivered strategic guidance to mature agency's defenses with effective detection, response, and recovery mechanisms; prepared for security service provider onboarding and managed the cybersecurity lifecycle.
- **Operational Cybersecurity Excellence**: Elevated FISMA maturity levels through strategic leadership; enhanced agency cybersecurity operations with a proactive, risk-informed approach, laying a robust foundation for long-term security management and compliance.

AVANADE/ACCENTURE, RESTON, VA **AUGUST 2017 – FEBRUARY 2019**
MANAGER INFORMATION SECURITY CONSULTING
***Avanade** is a professional services company with 50,000+ employees and $2 billion in revenue. It partners with its parent company, Accenture, a Fortune 500 company with $65 billion in revenue.*

I directed the Microsoft Azure Fed Cloud Team, managing the onboarding and training of new Gov Cloud Ops support members. I was crucial in coordinating with legacy vendors to support project growth and optimize the Ops SRE team for 24/7 incident and problem management across multiple locations. My responsibilities extended to program and project management of ten-million-dollar initiatives, overseeing finances, resources, and strategic planning. Additionally, I conducted thorough assessments of operations, security, and compliance processes within FEDRAMP guidelines, identifying vulnerabilities and implementing effective mitigation and 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.

I developed proof-of-concept dashboarding capabilities with PowerBI to provide SIEM-like functionality for cloud-native Azure clients. I took logs and machine status updates to create the needed dashboard around system availability and resilience status.

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

CTCA was a 5000+ stakeholder organization with over 2 Corporate offices and 5 Advanced Cancer Treatment Hospital systems. It was acquired by City of Hope in 2022.
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 security culture. I also consult on information security, assurance, and risk management during new project creativity and development with business units. I 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" and "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
Spearheaded the development of a 340+ hour holistic cybersecurity workforce development program for transitioning veterans and others into the cybersecurity industry. Collaborated with employers, educational organizations, and local/state agencies on the academic demands for employee attraction and retention.