Chad D. Freese

THIRD PARTY INFORMATION SECURITY RISK PROFESSIONAL

chad@chadfreese.com Cave Creek, AZ 850-529-6982

Profile

A diligent and highly skilled Third Party Information Security Risk Professional with 19 years of expertise in risk management, information & cyber security, and regulatory compliance.

Employment History

Quality Assurance & Tools Development Lead, USAA, Phoenix, AZ

June 2022 — Present

- Spearheaded the resolution of a Due Diligence Assessment (DDA) issue flagged by Enterprise Compliance/SLOD by meticulously re-engineering the DDA scoring guidelines, ensuring seamless alignment with our vendor control testing and pertinent evidence evaluations.
- Orchestrated and executed four rigorous control tests encompassing 120 assessment samples, with over 600 artifacts scrutinized, culminating in a flawless 100% pass rate with zero discrepancies identified.
- Championed and conducted 700+ Quality Assurance (QA) reviews of risk assessments, pinpointing and rectifying over 90 defects, thereby elevating the precision of each assessment prior to final examination and approval by control partners, auditors, and/or regulators.
- Directed and performed 72 meticulous Quality Assurance (QA) reviews during the re-scoring of 36 assessments, leading to an augmentation in Quality Risk Management (QRM) scores, thereby bolstering our team's Key Risk Indicator (KRI) metrics significantly.
- Engaged stakeholders in developing the CISO Dashboard for senior leadership, showcasing key metrics related to third-party risk assessments and improving executive insight regarding our risk posture.
- Pioneered a cost-cutting initiative that transitioned approximately 70+ onsite assessments to virtual platforms, carving out an impressive savings of ~$259,200 for the enterprise, all while adhering rigorously to TPRM's mandates and without amplifying risks. This initiative encapsulated a risk-based approach for both Net New vendors and Cyber Critical/High vendors, underscoring our adeptness in adapting innovatively without jeopardizing security or regulatory accord.
- Headed a high-priority virtual risk assessment for a Fortune 20 Company, efficiently averting the necessity for an onsite visit and unlocking substantial cost savings of around $40,000. By subverting the typical onsite support costs of approximately $4,000 per person per day over a two-day engagement, this innovative strategy underscored our fiscal prudence and resourcefulness while preserving the integrity of our risk posture at USAA.
- Served as a pivotal conduit for critical projects, offering timely and adept communication to stakeholders and assuring all concerns were tackled promptly and professionally.

- Utilized adept critical thinking and honed expertise in data analysis tools including RSA Archer, Enlighta, and Salesforce to craft and disseminate comprehensive risk reports. These instrumental reports, advocating a data-driven, risk-based strategy, informed and catalyzed discerning decision-making among leadership tiers up to the CISO, engendering pivotal strategic augmentations in our risk management architecture.
- Dedicated approximately 30 hours executing an exhaustive alignment and gap analysis between TruSight's Best Practice Questionnaire (BPQ) and USAA InfoSec's Due Diligence Questionnaire (DDQ), which propelled the efficiency and throughput of third-party risk assessments substantially.
- Rectified 8 defects identified during audits and by SLOD teams regarding various assessment discrepancies, ensuring an unblemished 100% accuracy rate in our team's TPCRA DDAs.

Lead Information Security Advisor, USAA, Phoenix, AZ

November 2019 — Present

- Spearheaded third-party risk assessments by fostering collaborative engagements with internal partners like third-party relationship managers, and second and third-line risk and compliance auditors, as well as external partners including vendors and C-Suite executives. Thrived in a highly collaborative and effective environment, ensuring a harmonized approach towards comprehensive risk management and compliance adherence.
- Performed over 300 information security risk assessments of varying complexity for dynamic projects, technologies, environments, business partners, and third parties throughout the financial and tech industries.
- Drafted enterprise-level requirements for the on-boarding and integration of a new Governance, Risk, and Compliance (GRC) tool, enhancing system security configurations and risk mitigation effectiveness while increasing operational efficiency by 35%.
- Developed 29 Quick Reference Guides (QRG) and recorded 27 hours of instructional videos, increasing the efficiency of onboarding, training, and standardized operating procedures throughout the enterprise.
- Formed partnerships with internal and external Cyber Threat Intelligence (CTI) teams, producing over 75 Intelligence Reports that directly contributed to the reduction of enterprise cyber risk by 27%.
- Developed, published, and maintained complex Information Security governance (e.g., policies, principles, standards) that define Information Security requirements.
- Served on Shared Assessments Standardized Control Assessments (SCA) Committee providing guidance in the security tenets of Physical Environment, Server Security, Network Security, Cloud Security, and Threat Management.

Principal Cybersecurity Architect & Red Team Lead, Honeywell Aerospace, Phoenix, AZ

October 2018 — October 2019

Responsible for the secure design and testing of safety-critical systems and communication assets for the commercial aerospace industry and the National Aeronautics and Space Administration (NASA).

- Led a team of engineers, spread across 3 continents, fostering a highly collaborative environment to drive product supply chain development forward while identifying, managing, and communicating challenges to management, resulting in positive business outcomes.
- As a co-inventor, submitted three patent applications aiming to solve common complex Aerospace engineering problems with innovative solutions.

- Led and co-authored a Product Security Guidelines (PSG) handbook for engineering teams to ensure systems security is woven throughout the entire Systems Development Life Cycle (SDLC), from concept to market.
- Served as a key stakeholder in the development of the cybersecurity team's penetration testing and vulnerability assessment roadmap and capabilities for Honeywell Aerospace's product teams, including the Connected Aircraft, with specific regard to SATCOM, GPS, and cellular communications.

Cyberwarfare / Computer Network Exploitation (CNE) Officer, United States Marine Corps & National Security Agency (NSA), U.S. & Middle East

2004 — October 2018

- Retired Chief Warrant Officer 3, USMC
- Served in many technical billets throughout the U.S., Iraq, and Afghanistan, all *Top Secret*, supporting the Marine Corps, NSA, and multinational Intelligence Community.
    - Information Security Officer
    - Information Systems Engineer
    - Information Technology Instructor, Course Chief, & Curriculum Developer
    - Cyberwarfare / Computer Network Exploitation (CNE) Officer
    - Signals Intelligence Officer
- Directly responsible for oversight and compliance with all state, federal, and international laws, rules, and regulations.
- Managed and operated a $38 million cellular telecommunications network and virtual cyberspace training environment comprised of over 6,000 end items, creating a multi-tiered, cross-platform-compatible, adaptable, wireless telecommunications system. This system support service-level training exercises, providing an Opposing Force communications environment for the tenets of Signals Intelligence, Electronic Warfare, and holistic Cyberspace Operations.
- Led a collaborative project with the Office of Naval Research (ONR), Massachusetts Institute of Technology Lincoln Laboratory (MIT-LL), and Johns Hopkins' Applied Physics Laboratory (APL) on the development of a multi-million-dollar Tactical Cyber Range (TCR) to train and certify Marines on full-spectrum cyberspace operations, from the national to the tactical edge.
- Developed a state-of-the-art Joint Cyberspace Operations Lab for the employment and testing of Offensive and Defensive Cyberspace Operations (OCO/DCO) tactics, techniques, and procedures (TTPs). This lab was engineered with no cost to the command while valued over $400,000.00.
- Designed and configured a state-of-the-art wireless network training lab, enabling the development of multiple training scenarios allowing for flexibility and realism utilizing a combination of virtual and physical environments comprised of over 30 cyber personas, 50 client devices, 45 mobile devices, 20 servers, and 15 Wireless Access Points (WAPs), using a wide variety of desktop and mobile operating systems, with a total system valuation over $1.8 million.

Education

Master of Science in Cybersecurity, Liberty University

- Graduated with Distinct Honors

Bachelor of Science in Information & Computer Science, Park University

- Graduated with Distinct Honors
- Emphasis in Networking & Security Engineering

Skills, Tools, Frameworks, & Regulations

Servant Leadership

Third Party Risk Management

Information & Cyber Security Risk Assessments

Regulatory Compliance

Effective Communication

RSA Archer / Eagle Eye

JIRA & Asana

Shared Assessments

TruSight

OCC Bulletin 2023-17

ISO/IEC 27001:2013

Payment Card Industry Data Security Standard (PCI DSS)

Conflcit Resolution

Third Party Risk Assesment Lifecycle

Governance, Risk, & Compliance Oversight

Leadership & Team Building

ChatGPT, Google Bard, Bing Chat AI Tools

Salesforce

Enlighta

BitSight

SOC2 Type II

23 NYCRR 500

NIST 800-53

NIST Cybersecurity Framework (CSF)

Certifications

• Certified Information Systems Security Professional - CISSP

• Certified Regulatory Vendor Program Manager - CRVPM III

• Certified Third-Party Risk Assessor - CTPRA [Oct 23]

• CompTIA Secure Cloud Professional – CSCP

• Certificate of Cloud Security Knowledge - CCSK v.4

• Google Cloud Certified - Cloud Digital Leader

• Microsoft - Essentials in Generative AI

• CompTIA Cloud+

• CompTIA Pentest+

• CompTIA Security Analytics Expert - CSAE

• CompTIA CySA+

• Certified in Risk and Information Systems Controls - CRISC

• Certified Third-Party Risk Professional - CTPRP

• Certified Data Privacy Solutions Engineer - CDPSE

• Certified Cloud Security Professional - CCSP

• AWS Certified Cloud Practitioner - CCP

• Google Cloud Certified - AI Fundamentals: Machine Learning & AI

• CompTIA Cloud Admin Professional – CCAP

• Certified Ethical Hacker - C|EH

• CompTIA Network Vulnerability Assessment Professional - CNVP

• CompTIA Security Analytics Professional – CSAP

• CompTIA Security+

• CompTIA Network Security Professional - CNSP

• CompTIA Secure Infrastructure Expert - CSIE

• Certified Information Privacy Professional - CIPP/US [Oct 23]

• CompTIA Advanced Security Practitioner - CASP+

• CompTIA Network Infrastructure Professional – CNIP

• CompTIA Network+

• CompTIA Server+

Industry Involvement

Marine Corps Cyber Auxillarist

March 2020 — Present

Volunteered over 50 hours mentoring Active-Duty Marines through the Marine Corps Cyber Auxiliary program, providing training, education, and mentorship with an end state of increased operational combat readiness for Marines to keep pace with constantly evolving cyber challenges.

Committee Member, Shared Assessments

November 2019 — Present

Tools & Emerging Technologies

Provide guidance and technical expertise for the ongoing development of the Standardized Control Assessments (SCA) and Standardized Information Gathering (SIG) tools, providing guidance in the following security tenets and risk domains: Security Policy, Organizational Security, Physical and Environmental Security, Network Security, Privacy, Threat Management, Server Security, Artificial Intelligence, and Cloud Security.

Contributing Member, Infragard, Phoenix Chapter, Phoenix, AZ

2018 — Present

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. I specialize in the following sectors: Communications, Defense Industrial Base, Financial Services, Information Technology, & Transportation Systems.

Patents & Publications

Mobile Device Authenticator, Phoenix, AZ

October 2019

Co-Inventors: Andrew Wise; Praveen KR

Copyright: Honeywell International, Inc.

View Here

PSYOP, Deception, And Cyberspace In the Open: Analysing Fake News In The Open, Twentynine Palms, CA

June 2017

Co-Authors: Terry Traylor; William Wong

View Here

Links

Professional Portfolio (chadfreese.com) LinkedIn