

Christopher Green

Cybersecurity & GRC Consulting | Information Security Leadership | Technology Risk & Compliance

CISSP | CISA | CRISC | PCI QSA | OSCP | CMMC RP

Brooklyn, New York, USA | Open to relocation to Dublin, Ireland

iamchrisgreen@gmail.com | +1 503 867 0858 | linkedin.com/in/christophermgreen

Eligible for Irish Critical Skills Employment Permit

PROFESSIONAL PROFILE

Cybersecurity consulting leader with 12+ years of experience in IT security and 8+ years of experience delivering governance, risk, and compliance programmes across heavily regulated industries including financial services, healthcare, utilities, and critical infrastructure. Brings a strong foundation in information security controls, technology risk, and regulatory compliance, with experience advising clients operating under complex, multi-jurisdictional obligations including PCI DSS, HIPAA, DORA, NERC CIP, and CMMC. Has supported organisations with transatlantic operations in understanding where GDPR intersects with their information security and control frameworks, providing advisory-level guidance on alignment. Experienced in leading client-facing engagements from scoping and discovery through to remediation roadmaps and board-level reporting, and in building and developing teams of consultants to deliver high-quality, risk-based work under tight timelines. Combines deep technical security expertise with a proven ability to translate complex regulatory and threat-landscape developments into clear, business-relevant narratives for executive, audit committee, and board audiences. Holds CISSP alongside CISA and CRISC, and is a regular conference speaker on governance, risk, and compliance in regulated environments.

KEY CAPABILITIES

Cybersecurity & GRC Consulting | Information Security Controls Assurance | Technology Controls Assurance & Testing

ICT Risk Framework Development | Regulatory Compliance & Maturity Assessments | Remediation Programme Design & Roadmapping

Client Engagement & Trusted Advisory | Board & Executive Reporting | Third Party & Vendor Risk Management
Team Leadership, Coaching & Development | Public Speaking & Thought Leadership | Offensive Security & Control Validation

FRAMEWORKS & STANDARDS

Privacy & regulatory exposure: GDPR (advisory-level, transatlantic clients); HIPAA Privacy and Security Rule (GRC advisory context).

Cybersecurity & GRC: NIST CSF v2, NIST SP 800-53 and 800-171, NIST SP 800-30; CIS Critical Security Controls v8; ISO/IEC 27001 and 27002; PCI DSS 4.0.1 (QSA certified); CMMC; SOC 2 (SSAE 18) attestation readiness.

Additional exposure: DORA (Digital Operational Resilience Act); NERC CIP; MITRE ATT&CK; Enterprise Risk Management frameworks.

PROFESSIONAL EXPERIENCE

Director of Governance, Risk & Compliance

Structured Communication Systems, Inc. | New York City | March 2026 to Present

- Lead the firm's GRC consulting practice, directing a team of assessors and penetration testers delivering compliance programme design and control assurance across financial services, healthcare, utilities, and critical infrastructure clients.
- Act as trusted virtual CISO and risk advisor to multiple clients, guiding information security governance, regulatory alignment, and board-level risk reporting across cybersecurity and compliance domains.
- Translate complex regulatory developments including DORA, HIPAA, NERC CIP, and CMMC into practical programme enhancements, remediation roadmaps, and executive-ready risk narratives tailored to client operating contexts.
- Lead the firm's SOC 2 (SSAE 18) attestation programme, overseeing control design and remediation, evidence preparation, and direct engagement with the external auditor across security and availability domains.

- Design and deliver multi-year remediation roadmaps aligned to NIST CSF v2, NIST SP 800-53, ISO 27001, and applicable regulatory frameworks, scoping enhancement programmes and tracking progress against control maturity targets.
- Build productive, trusted relationships with client audit, compliance, legal, procurement, and risk teams, embedding information security and data governance considerations into operational processes and governance structures.
- Own presales and service development for the GRC portfolio, expanding offerings into AI security assurance, third party risk management, OT/ICS security, and data governance advisory.
- Present risk findings, programme recommendations, and security roadmaps to executive leadership and boards, tailoring content and tone to non-technical stakeholders.

Manager, Penetration Testing & Virtual CISO Services

Structured Communication Systems, Inc. | New York City | September 2023 to March 2026

- Acted as virtual CISO for multiple clients across financial services, healthcare, and critical infrastructure, advising on information security governance, regulatory compliance, and security programme maturity.
- Designed and delivered risk-based control assessments aligned to NIST CSF, NIST SP 800-53, ISO 27001, and applicable regulatory frameworks, documenting control gaps, remediation plans, and residual risk in formal client-facing assurance reports.
- Delivered PCI DSS assessments as a Qualified Security Assessor (QSA), evaluating control design and operating effectiveness and producing Reports on Compliance (ROCs) and Self-Assessment Questionnaires (SAQs).
- Led and developed a team of penetration testers, coaching both technical delivery and the ability to communicate complex findings to executive, legal, and operational audiences with clarity and appropriate context.
- Partnered with client audit, compliance, procurement, and legal teams to support regulatory enquiries, client assurance submissions, and remediation governance activities.
- Interpreted threat intelligence, assessment findings, and control evidence to produce robust, risk-based conclusions and translate them into prioritised programme recommendations for senior stakeholders.
- Identified and developed sales opportunities, contributing to proposals and go-to-market activity across data protection, privacy, and broader cybersecurity consulting services.

Security Engineer & Penetration Tester

Structured Communication Systems, Inc. | USA | August 2018 to August 2023

- Performed technology risk assessments and control effectiveness reviews across cloud and hybrid environments following NIST SP 800-30 methodology, covering information security and applicable regulatory control requirements.
- Led PCI DSS readiness, remediation, and QSA assessment delivery, validating the design and operating effectiveness of cardholder data environment controls.
- Developed and maintained information security policies, standards, and procedural content aligned with NIST SP 800-53 and ISO 27001, translating control requirements into accessible, operationally relevant guidance.
- Supported external audits and client-driven assurance activities through control testing, evidence collation, and remediation tracking across SOC, PCI DSS, and regulatory review processes.
- Translated technical findings into business-relevant, risk-based reporting for non-technical stakeholders, ensuring clarity of impact and prioritisation at executive level.
- Acted as first responder for client security incidents, conducting root-cause analysis, debriefing stakeholders, and reinforcing incident management practices.

MSP Lead Engineer

Structured Communication Systems, Inc. | USA | April 2018 to August 2018

- Led the transition of the practice toward a Managed Security Service Provider model, implementing continuous control monitoring, event correlation, and security best practice frameworks.
- Designed and delivered training on secure operations, incident response, and security awareness for internal staff and client teams, reinforcing consistent behaviours across diverse technical audiences.

MSP Systems Engineer (Tier 1 and Tier 2)

Structured Communication Systems, Inc. | USA | February 2013 to April 2018

- Maintained secure operations, vulnerability management, and configuration hardening across 40+ concurrent client environments, building a strong foundation in infrastructure security and operational risk management.
- Built and maintained enterprise network infrastructure including Fortinet, Palo Alto, Sophos, Juniper, Cisco, and Aruba, and deployed Windows Server environments across standalone, Hyper-V, and VMware platforms.

Manager

Regal Entertainment Group | USA | November 2000 to February 2013

- Built and maintained training strategies for a team of 30+ associate managers and floor staff, embedding consistent standards and behaviours across a fast-paced, customer-facing environment.
- Mentored and developed associate managers and front-line staff using an open-door leadership approach, building individuals into stronger performers and future leaders.

THOUGHT LEADERSHIP & EXTERNAL ENGAGEMENT

- Regular conference speaker on information security governance, risk and compliance in regulated environments, PCI DSS and payment security, and practical GRC programme implementation.
- Trusted presales and client-facing advisor on security programme maturity, ICT risk, and regulatory compliance, with a track record of converting advisory conversations into sustained consulting engagements.
- Contributor to security culture and awareness initiatives through executive briefings, board presentations, workshops, and written thought pieces on emerging regulatory and threat topics.

CERTIFICATIONS

CISSP (Certified Information Systems Security Professional)

CISA (Certified Information Systems Auditor)

CRISC (Certified in Risk and Information Systems Control)

PCI QSA (Qualified Security Assessor) & PCIP (Payment Card Industry Professional)

OSCP (Offensive Security Certified Professional)

CMMC RP (Cybersecurity Maturity Model Certification Registered Practitioner)

EDUCATION

Bachelor of Science, Data Communications Systems Technology & Computer Networking

ITT Technical Institute, Portland, Oregon, USA | 2008 to 2011

ADDITIONAL INFORMATION

- Available for relocation to Dublin, Ireland; eligible for Irish Critical Skills Employment Permit (ICT/cybersecurity category).
- Experienced operating across blended, remote, and internationally distributed consulting teams.
- Strong written and verbal communication skills across technical, executive, legal, and board audiences.