

John Rector, MDiv, MSIA, BSBA, PMP, CISSP, CGRC, CCP, ITIL, FITSP-M, MCSE, MCDBA, A+

Enterprise Governance | AI & Automation Strategy | Digital Modernization | Operational Resilience
Active TS/SCI with CI Polygraph | U.S. Citizen

RectorResume@gmail.com | linkedin.com/in/john-rector/

Executive Profile

Executive governance, cybersecurity, and technology modernization leader with 30 years of experience driving enterprise transformation, operational resilience, and scalable assurance programs across federal, defense, financial, and commercial environments. Proven record aligning governance, enterprise architecture, automation, and data-driven operations to improve organizational resilience, risk visibility, and business performance at scale. Trusted advisor to executive leadership on enterprise risk, modernization strategy, Zero Trust architecture, operational continuity, and compliance transformation supporting budgets exceeding \$3B and protection of financial transactions exceeding \$2.3T annually. Recognized for building engineering-driven governance capabilities integrating cloud platforms, continuous monitoring, AI-enabled analytics, automation, and policy-driven security architectures to strengthen enterprise resilience and accelerate measurable business and mission outcomes.

Core Competencies & Leadership Focus

- Enterprise Governance & Assurance | Executive Risk Management | Operational Resilience | Board & C-Suite Advisory | Cross-Functional Leadership | Organizational Transformation
- Governance Engineering | Compliance Automation | Continuous Monitoring | Zero Trust Architecture (IT & OT) | Cloud & Platform Security | AI-Enabled Analytics & Automation
- Enterprise Assurance | Cybersecurity Strategy | Integrated Risk Management | Identity & Access Governance | Vulnerability & Threat Management
- CMMC | RMF/CSF | FedRAMP | PCI DSS | SOX | GLBA | ISO 27001 | Data Governance & Privacy

Career Highlights

- Led enterprise governance, cybersecurity and operational resilience initiatives across federal, defense, financial, healthcare, and commercial environments supporting large-scale mission-critical operations.
- Built and scaled engineering-driven governance and assurance capabilities integrating automation, telemetry, continuous monitoring, and AI-enabled analytics to improve enterprise risk visibility, audit readiness, and operational effectiveness.
- Directed enterprise modernization and Zero Trust transformation initiatives, strengthening operational resilience, adaptive security capabilities, and protection of critical infrastructure.
- Advised executive leadership stakeholders, translating complex cybersecurity, governance, and modernization challenges into scalable business and mission outcomes.
- Developed enterprise governance operating models and integrated risk management capabilities aligned to RMF, NIST, PCI DSS, SOX, GLBA, HIPAA, FedRAMP, and state and federal privacy requirements across highly regulated environments.
- Led multidisciplinary cybersecurity, governance, architecture, engineering, and operational teams supporting distributed enterprise environments, large-scale modernization programs, and high-consequence national security operations.

Professional Experience

Director, Technology Business Line & GRC, CTO | Chinook Systems, Inc. | Arlington, VA | 2024 – Present

- Own enterprise technology, cybersecurity, governance, risk, and compliance functions, aligning modernization, operational resilience, and cyber governance across highly regulated environments.
- Lead high-performing teams and scalable governance operating models integrating engineering, security, compliance, and operational stakeholders to improve enterprise accountability, accelerate decision-making, and support organizational growth in rapidly evolving environments.
- Direct enterprise governance modernization initiatives integrating IT/OT Zero Trust, cloud-native security, policy-driven controls, adaptive access enforcement, and continuous monitoring to strengthen operational resilience and mission continuity.
- Architected engineering-driven assurance capabilities leveraging automation, telemetry, AI-enabled analytics, automated evidence collection, and continuous controls validation to improve enterprise risk visibility and reduce compliance overhead.
- Established scalable compliance and assurance processes aligned to CMMC Level 2, NIST RMF, NIST 800-171, Zero Trust, and enterprise data protection requirements governing CUI, FCI, and PII.
- Partner with executive engineering and operational leadership to align enterprise technology investments, secure system design, modernization priorities, and governance strategy with business growth and risk management objectives.
- Direct secure digital transformation initiatives embedding governance, AI, automation, behavioral analytics, and operational visibility into cloud-native and mission-critical enterprise environments.
- Maintain accountability for technology governance, cybersecurity investment strategy, operational performance, executive risk reporting, and cross-functional modernization efforts supporting organizational resilience and growth.

Enterprise Risk Advisory & Governance Lead, CISO | NXT | North Bethesda, MD | 2022 – 2024

- Owned enterprise governance, cyber risk, operational resilience, and modernization initiatives supporting large-scale state government and regulated sector environments.
- Advised Maryland Governor, DoIT Executive Leadership and affiliated agencies on enterprise risk, governance, modernization strategy, and continuous monitoring initiatives.
- Led development of scalable governance operating models integrating enterprise telemetry, risk analytics, automated assurance processes, continuous monitoring, and analytics-driven security modernization capabilities.
- Built cross-functional governance and assurance partnerships across engineering, security, compliance, and executive stakeholders to improve accountability and enterprise risk visibility.
- Directed implementation of integrated risk management capabilities including ServiceNow GRC, identity governance, privileged access management, continuous authority-to-operate processes, and enterprise monitoring strategies aligned to CSF, HIPAA, and state privacy requirements.
- Led governance and executive risk evaluations, third-party audit reviews, vendor risk analysis, and enterprise architecture assessments across hybrid cloud and distributed operational environments.
- Directed and mentored multidisciplinary cybersecurity and governance teams while advising executive stakeholders on governance modernization, operational resilience, emerging threats, and AI-enabled security capabilities.

Founding Partner, CISO | SVD Solutions | Washington, DC | 2011 – 2022

- Founded and led a consulting organization supporting federal, defense, intelligence, and commercial clients operating in highly regulated and mission-critical environments.
- Directed cybersecurity strategy, enterprise risk management and governance programs across organizations including FBI, SEC, IRS, U.S. Army, U.S. Air Force, and commercial enterprise clients.
- Advised executive leadership, translating cybersecurity, governance, Zero Trust, and operational resilience requirements into scalable enterprise modernization strategies.
- Built multidisciplinary engineering and governance teams supporting national security, investigative, geospatial, telecommunications, and enterprise operational environments.
- Established scalable governance and operational assurance models integrating engineering, security, compliance, and executive stakeholders to improve accountability, audit readiness, and enterprise risk visibility across complex client environments.
- Led RMF modernization and architecture-first compliance initiatives integrating automated evidence collection, telemetry-driven assurance, continuous monitoring, and control validation capabilities to improve audit readiness and enterprise risk visibility.
- Architected advanced cloud, hybrid, and intelligence platform architectures leveraging AWS, Azure, Zero Trust, FedRAMP-aligned principles, centralized telemetry, analytics-driven monitoring, and automated response orchestration.
- Developed executive cyber risk visibility, governance reporting, and operational analytics capabilities supporting strategic modernization initiatives across mission-critical environments.
- Oversaw strategic program delivery, customer engagement, organizational growth, and operational performance across a broad portfolio of enterprise modernization and cybersecurity initiatives supporting long-term client retention and expansion.

Earlier Roles (1994 – 2011)

Cyber Program Director | Quotient Inc. | 2010-2011

- Directed DISA PEO-MA cybersecurity initiatives securing the global .mil DNS infrastructure and supporting enterprise resilience for Department of Defense communications environments.
- Led cross-functional engineering and security teams advancing secure BIND architecture, operational governance, vulnerability reduction, and scalable DNS security capabilities supporting worldwide deployment.
- Partnered with DoD, USCYBERCOM, NSA, and enterprise stakeholders to strengthen operational assurance, security architecture, and governance alignment across distributed federal infrastructure environments.

Sr. Manager | Phase One Consulting Group (now Accenture) | 2008-2010

- Directed enterprise cybersecurity transformation and governance initiatives supporting U.S. Army CIO G-6, DoT, DOI, CFTC, and other federal portfolios exceeding \$3B in combined operational scope.
- Led enterprise cyber modernization efforts integrating ITIL, COBIT, NIST, and operational governance frameworks to improve enterprise risk visibility, audit readiness, and cross-organizational security alignment.
- Built an executive cyber risk dashboard and enterprise metrics capability enhancing operational visibility, governance reporting, and strategic decision-making for senior military leadership.

Sr. Manager | Delta Solutions & Technologies (now CACI) | 2006-2008

- Supported enterprise security and governance strategy for the Department of the Interior's \$1.2B SAP modernization initiative consolidating 86 legacy systems into a unified enterprise platform.
- Led governance, PMO coordination, and SOX separation-of-duties initiatives supporting enterprise modernization, financial systems transformation, and operational risk reduction across large-scale federal environments.

Global Information Security Manager, First Data Corp. | 2001-2006

- Directed global information security governance and operational assurance initiatives supporting more than \$2.3T in annual financial transactions across First Data, Western Union, TeleCheck, and international business operations.
- Governed enterprise security and compliance programs aligned to PCI/CISP, GLBA, SOX, HIPAA, SAS 70, and international privacy requirements across North America, Europe, Australia, and UK operations.
- Led enterprise security architecture reviews, governance modernization efforts, and consensus-driven policy initiatives strengthening protection of global financial systems and distributed operational environments.
- Designed and operationalized enterprise security testing and forensics capabilities leveraging automated vulnerability analysis, continuous assessment methodologies, and advanced investigative tooling to significantly reduce enterprise risk exposure.
- Oversaw integrated operational security functions including physical security governance, surveillance systems, datacenter protection, and enterprise access control operations supporting resilient global business operations.

Manager, Global Support, Universal Computer Systems (now Reynolds & Reynolds) | 1998-2001

- Directed global operational technology support and enterprise infrastructure modernization initiatives, implementing Active Directory transformation, centralized monitoring, SIEM visibility, and operational process improvements across multinational environments.
- Led technical operations and engineering teams improving enterprise uptime, operational scalability, and security visibility through integrated monitoring and support modernization efforts.

Various commercial marketing firms – Early career included digital marketing and creative technology roles focused on graphics, layout, web development, and client-facing visual solutions.

Education & Certifications

- M.Div., Theology – Liberty University (Summa Cum Laude) - 2019
- M.S., Information Assurance – Norwich University (4.0 GPA) - 2006
- B.S., Business Administration – University of Phoenix (Cum Laude) - 2004

PMP, CISSP, CGRC, CCP, ITIL, FITSP-M, MCSE, MCDBA, A+, GitHub Foundations. Claude Certified Architect – Professional (CCAR-P) in progress. Expired: CCNA, CCDA | Active TS/SCI with CI Poly

Publications

- Visit JohnRector.com to view