Richard Kaplan

Senior Consultant IT Governance Risk And Compliance @ SVB / Boston Private Bank

Email: c2m-3my-mx8@mail.dice.com
Phone: 6092355555

Summary

Previous	Senior Consultant Governance Risk And Compliance Enterprise @ Vanguard Financial Services
Preferred	Senior IT Governance Risk Compliance SVP Director
Location	Plainsboro Township, NJ, US
Desired Work Settings	No Preference
Willing to Relocate	No
Work Authorization(s):	Authorized to work in the United States on a full-time basis.
Security Clearance Info:	US Citizen (for security purposes)
Employment Type	Full-time Contract - Independent Contract - W2 Contract to Hire - Independent Contract to Hire - W2
Total Experience	31 years
Education	Bachelors @ Monmouth University
Profile Source	Dice
Profile Downloaded	Monday, December 9, 2024

Richard Andrew Kaplan
27 Franklin Drive ● Plainsboro, NJ 08536

●

Summary:	Experienced executive level cybersecurity IT Governance Risk & Compliance leader who develops, manages, provides oversight, and executes IT risk & compliance programs, information security and IT risk projects including regulatory IT audits, technical vulnerability assessments, secure disaster recovery/business continuity, and technology implementations
Expertise:	IT Risk & Compliance, Governance, IT Risk Program, IT Risk Assessments, Risk Exception Management, security policy design and management, business continuity and disaster recovery, secure SDLC, Data Loss Prevention, and information security strategy, Cloud Security, Incident Response, Change of Custody, Encryption Management, Patch and Vulnerability Management

Organization Leadership
- IT Risk Director
- Senior IT Risk & Compliance Consultant

Project Leadership
- Risk Management
- IT Compliance and Governance
- Project Management
- Problem Management & Root Cause Analysts

Standards, Frameworks, & GRC
- Cloud Security Alliance, CMMI, COBIT, COSO, DOD 8500.2,FAIR, FedRAMP, FFEIC, FISMA, GDPR, GLBA, HIPAA,HITRUST, ISO 25010, 27001, 27005, ITIL, ITAR, NIST , 800-53, PCI, SABSA, SOX, TOGAF, VISA 3DS
- ServiceNow, RSA Archer, DLP, Symantec CCS, OCTAVE-S, GRC custom tools

Business Sectors
- Financial, Healthcare, Technology

Technologies
- Cloud: Microsoft Azure, AWS, SaaS, IaaS, DRaaS
- Security Monitoring: Networking – CrowdStrike, FireMon, SolarWinds, SIEM – ArcSight, Splunk, Envision, SA
- Security Devices: HSM, Thales, SafeNet,F5
- Attack Prevention: DDOS, intrusion Detection and Prevention (IDS, IPS) patching, phishing
- Operating Systems: Windows, Linux, legacy operating systems.
- Databases: Microsoft Access, Microsoft SQL, Oracle, FileMaker Pro, and others.
- Office Application Software: ServiceNow, Jira, Microsoft Exchange, SharePoint, Confluence, Orbus iServer, MSFT Teams, and others.
- Financial: Crystal Reports, Sage MAS 90, Oracle

Experience

Senior Consultant – IT Governance Risk and Compliance
Silicon Valley Bank / Boston Private Bank
Boston, Massachusetts   2019 to Present

Leadership
- Provide leadership and managerial guidance in the remediation of high exposure and other IT Risk projects potentially affecting the Bank's IT risk posture within all infrastructure services.
- Develop IT risk program to lead improvements within multiple IT services establishing a robust IT risk framework that identifies and mitigates current as well as emerging risks.
- Provide thought leadership to the business and IT risk & control owners. Contribute to the ongoing remediation work, including bringing industry perspectives, and guidance on developing it risk management frameworks to further enhance the operating model.
- Act in a Chief of Staff capacity managing project work across multiple teams, including budgeting, planning, and plan execution activities.
- Innovate and develop methods to make the function more efficient and ensure local processes are considered in global initiatives all within an align risk management perspective.
- Collaborate with internal and external audit teams to ensure compliance with all requirements and timely responses to queries.

- Guide multiple global teams focused on IT control, monitoring exception reports, data quality oversight and control reporting.
- Facilitate accurate and appropriate reporting of operational risks caused by technology to senior management and various senior risk forums.
- Participate in regional and global IT risk and control committee meetings, IT DR, IT BCP, IT incident, IT Asset Management, Change Management, risk and control committee meetings.

Governance
- Develop, and optimize essential IT programs under infrastructure which includes IT Asset management, IT incident Management, IT Problem Management, IT DR, IT BCP, and IT Architecture.
- Develop and enhance global IT directives (Policies, standards, SoPs) with control owners. Provide guidance on standardization, awareness, implementation assistance, and enforcement.
- Develop reporting and tracking of key issues, MRA status and Control KRIs. Develop regional / global KRIs and ensure function heads have an adequate control clear view dashboard of ongoing risks/issues and remediation work
- Review process changes/implementation which may impact controls

Operations
- Build out and optimize multiple ITIL related services including IT Asset Management, IT Incident Management, IT Problem Management, Change Management, Disaster Recovery, Business Continuity within their perspective phase/life cycle.
- Ensure compliance with the Bank's Information Technology and Information Security directives.
- Guide IT team to pro-actively identify Risk and Control gaps/ weaknesses and provide practical recommendations to improve the quality and effectiveness of the control environment.
- Collaborate with colleagues in other areas of Risk Management, Finance, Compliance/ Control, and the Businesses to assure appropriate management of Technology Risk processes.
- Facilitate accurate and appropriate reporting of Technology risk / Technology Key Risk Indicators to regional and global senior management.
- Identify emerging Technology risks in the context of the current economic, regulatory, and business environment and assure that measures are being taken to mitigate these risks.
- Analyze Technology risk data (typically losses, metrics, or assessment results) to identify areas of excessive risk and to ensure that mitigation efforts are having the desired effect(s).
- Oversee, coordinate, present remediation work and develop plans to close control gaps identified by internal and external assessors. Manage associated IT Risk Exceptions as needed.
- Plan and coordinate infrastructure on-going infrastructure project management work.
- Represent infrastructure at internal audit, third party IT risk, department committees.
- Build out and contribute to the evolution of the Infrastructure's IT service framework (ITIL).
- Ensure the organization's risk profile as related to its activities and dependencies are in alignment with the Bank's Business Strategy and Risk Appetite.
- Monitor and analyze IT risks within the infrastructure 's IT services and develop reporting on these risks to internal stakeholders.
- Act as the Subject Matter Expert for the design and implementation of strategic changes to infrastructure program and processes.
- Ensure IT Governance, Risk , & Compliance culture is positively impacted through effective training, support tools, and processes.
- Develop and mentor multiple department team members including Manage Service Provider (MSP) staff.

Senior Consultant – Governance Risk and Compliance Enterprise
Vanguard Financial Services
Valley Forge, Pennsylvania   2017 to 2019

- Developed and enhanced a world class Global Technology Office Enterprise Architecture – Governance, Risk, and Compliance program.
- Established program governance, maturity roadmaps with obtainable strategic objectives utilizing a hybrid best fit approach of industry frameworks and leading practices.
- Developed and enhanced Life Cycle Management program/practices for tracking, assessing, reporting, and governing components throughout the enterprise.
- Created and maintained global GRC policy management program, including developing the corresponding directives and operationalizing effective controls in accordance with business concerns and regulatory requirements.
- Collaborated with internal and external technology service groups to effectively monitor and remediate vulnerabilities within the environment to help ensure continuous compliance.
- Created and procured the tools to be used within the enterprise that improve operational efficiency, identifying risk points while providing corrective guidance to meet conformance objectives.
- Developed and improved enterprise architecture planning that focuses on delivering the strategic business capabilities and objectives of the enterprise in an acceptable risk tolerance approach.

Senior Consultant of SaaS Operations Risk & Compliance, IT Risk Management & Security
RSA, The Security Division of EMC, Dell Technologies

Bedford, Massachusetts   2014 to 2017

- Established, managed, and maintained the internal IT Cybersecurity risk and compliance program for global SaaS Operation's supported products and services.
- Oversaw strategic cloud based governance, risk, and compliance initiatives
- Acted as liaison between cross functional teams in communicating, demonstrating, implementing, and maintaining operational controls within the SaaS Operations environment.
- Worked with the technology owners to ensure the security controls are understood, implemented, tracked, and validated for audit review.
- Represented SaaS Operations in product development committees and other organizational strategic initiatives within SaaS environment regarding security, risk, and compliance requirements.
- Provided guidance regarding risk management within SaaS Operations to senior management.
- Helped ensure project compliance objectives, deliverables are understood and met by project resources.

Senior Consultant, IT Risk Management & Security, OpenSky Corporation
Princeton, New Jersey   2010 to 2016

- Assessed, developed, and improved enterprise IT risk & compliance management programs for global enterprise clients. Develop and implement comprehensive IT risk control frameworks based on regulatory requirements, existing policy/standards, business needs, and leading practices.
- Designed, oversaw, and supported key transformational projects, assessing security solutions to meet compliance and operational security needs and ensure that applicable

security solutions and technologies are implemented in a suitable and supportable manner to better enable and secure the business.

- Built and established third party risk assessment programs for multiple Fortune 100 companies to consolidate and manage third party risk across multiple divisions.
- Managed, developed, and conducted detailed IT risk assessments based on regulatory and leading practice requirements. Analyze and present to C-level management observation findings, qualitative and quantitative risks, potential impact to business, and recommended remediation plans.
- Designed, updated, and revised information security policies, standards, SOPs, and guidelines for large and small organizations across multiple industries. Utilize leading practices and industry standards in establishing a comprehensive, easy to comprehend process to control risk and facilitate company growth. Design, manage, and conduct global training and awareness classes on policy implementation and acceptance.
- Conducted and implemented strategic and operational level planning across the full spectrum of network and host-based cyber security. Translate corporate business strategies and environmental conditions into cyber security requirements, recommendations, designs and architectural roadmaps.
- Provided thought leadership to senior management around improving security operations. Act as a liaison between internal departments in communicating, demonstrating, implementing, and maintaining security controls within the operational environment.
- Provided technical guidance to senior management in a wide range of security issues including architectures, firewalls, electronic data traffic and network access. Provide implementation advice on leading data-at-rest and data-in-transit encryption technology, penetration and vulnerability analysis of various security technologies, and information technology security research.
- Created, and revised secure disaster recovery and business continuity plans for clients. Conduct, manage and coordinate DR annual testing. Establish and expand information security programs by integrating security processes and resources into existing DR infrastructure, application development, and financial departments.
- Developed, implemented, conducted, and managed regulatory IT assessment/audits for clients and third party providers. Present compliance reports to auditors and C-level management. Reports were used in evaluating and remediating risk findings.
- Designed security controls for major projects to be incorporated into applications, cryptography, operations, physical security, and system development.
- Established and managed IT security for clients. Ensure all infrastructure components (e.g. Firewalls, servers, workstations) adhered to security principles, policies and procedures.
- Acted as security lead and trusted resource for organizations to determine and manage the associated information security risks.

ERS Manager, Deloitte and Touche LLP
Princeton, New Jersey   2006 to 2009

Security and Risk Management
- Managed and performed IT security & compliance assessment projects for multi-billion dollar organizations to discover vulnerabilities, assess risk, and development remediation plans. Developed assessment approach and methodology that clients leveraged for future assessment projects.
- Managed and executed outsourcing and off-shoring risk assessments for global clients. Managed and performed security related IT projects for major healthcare and financial institutions, focusing on IT risk management, compliance, process improvement, information security strategy, internal assessments of technology operations, and logical access controls. Oversaw on-site assessments focusing on application development, maintenance and support, as well as security and internal controls of major outsourced providers throughout the world.

- Established remediation roadmap which allowed clients to allocate budgeted resources, time, and expenses required to remediate the control deficiencies. Managed security and privacy projects that determine whether the Information Technology security controls for clients were in place to secure data. Performed and developed vulnerability management solutions to proactively discover security deficiencies, and establish remediation plans to reduce exposure.
- Created and developed IT policies and Standard Operating Procedures (SOP) to build a comprehensive security program used by client's global organization. Conducted training classes on policy creation, maintenance, and review. Created database repository for managing policies. Established marketing campaign on socializing policies throughout the entire organization.
- Developed and proposed IT security application development solutions regarding authentication & authorization, auditing & logging, secure code review, encryption, and database security to be used for enterprise information security architecture methodology. Performed Business Risk Assessment, Applications Development Threat Modeling, and conducted training classes on application development security controls.
- Created, developed, and enhanced Disaster Recovery and Business Continuity Plans for small to global organizations. Ensured organization remains resilient to disruptions through the development and maintenance of a Business Continuity Management System with safeguards for end-to-end delivery of business critical products and services.
- Established curriculum and conducted IT security training classes to internal personnel and clients regarding leading security practices. Presented on-site and remote training to 50+ individuals regarding Certified Information Security Professional competencies including Software Development Life Cycle, and security policy, SOP, standards, and guideline development.

Technology Risk Management Professional, Jefferson Wells
Philadelphia, Pennsylvania   2005 to 2006
Security Assessments
- Conducted IT risk and compliance assessments for organizations in the financial and healthcare sector. Presented results to senior management and recommended solutions to remediate risks.
- Developed and presented a cost effective, efficient IT Risk Assessment Matrix tool for clients. The tools disclosed unknown technical vulnerabilities, and recommended corrective actions. The tool lowered their qualitative/quantitative risks, and improved their client relations.
- Created and completed a web configuration security audit for a multi-billion dollar financial institution. The findings and recommended corrective controls lowered the client's exposure and allowed expansion in web offerings.
- Created and developed Payment Card Industry (PCI) training classes for sales representation and clients on performing and assessing secure credit card transaction practices.
- Created an automated audit program used by professional staff to examine the controls and generate an approved audit approach. The tools saved the firm development time and kept deliverables in budget.

RAK Computer Consultants
Plainsboro, New Jersey   1993 to 2005

- Designed, conducted, participated and managed Sarbanes-Oxley audits for clients. Presented compliance reports to auditors and C-level management. Developed risk remediation roadmaps with milestones and deliverables to remediate findings.
- Established and managed IT security for clients. Ensured all desktops and servers adhered to security principles, policies and procedures. Implemented practices to avert possible disasters during critical production times.
- Designed security access controls for major projects that were incorporated into applications, cryptography, operations, physical security, and system development. Developed processes to improve security lowering expenses and increased profit margin.

- Developed client's intrusion detection system for monitoring internal and external internet activities. Incorporated preventative designs to lower downtime and increase processing accuracy for all divisions.
- Created detective systems to discover internal internet abuse, virus, worms, and Trojan horse attacks to increased client's productivity.
- Developed and participated in forensic crime detection, prevention, policy, and enforcement to prevented and reduced theft exposure for clients.

Management
- Managed an Identity Management project for a billion dollar manage care provider. Coordinated vendor and client relationship to ensure project kept on schedule. Reviewed and tested provisioning in six networking environments.
- Directed the expansion and supervision of the IT department team of 15 local and regional individuals. Responsible for client's computing, telephony, communications infrastructure and IT services. Annual budget responsibility: Over $10 million.
- Managed IT computing services for client's employees overseeing the HR software and services provided by the IT department. Services include: acquiring PCs; roll-out to users; remote helpdesk support; on-site desk side support for hardware and software; moves, adds and changes; and support for applications such as e-mail, file shares, electronic fax, and departmental programs.
- Managed the IT computing and communications infrastructure: data centers in multiple offices; LANs; multiple servers with data communications between offices and to the company's backbone network; and Internet connectivity.
- Managed vendor relationships. Select vendors; negotiating contracts and pricing; implementing vendor services and projects; and managing the day-to-day vendor relationship.

Mergers and Acquisitions / Divestitures
- Performed IT assessments of pending mergers related to information security, hardware, software, personnel, and provided recommendations for consolidation. Developed plans of consolidation plans of IT departments. Prepared operating budget for consolidation of IT departments. Developed training programs and conducted training programs to staff. These tasks assisted in expediting and orderly transition, maintaining policy/ standards/procedural compliance. These processes resulted in lower operational costs, and maintain IT aligned with business objectives.
- Developed plans for divesting IT departments. Assisted in the negotiation of IT outsourcing arrangements and Transition Services Agreements (TSAs). Divestiture included downsizing IT department technology and staff which allowed management flexibility to add/eliminate services, manage informational risk in a controlled manner, and improve exit strategy.

Project Management
- Consulted, facilitated, and managed multiple business continuity and disaster recovery projects, including Y2K preparedness, to mitigate probable interruptions.
- Managed an Identity Management project for a billion dollar managed care provider. Coordinated vendor and client relationship to ensure project kept on schedule. Reviewed and tested provisioning in six networking environments.
- Lead project management for multiple network migrations throughout the country. Incorporated new sites into existing Wide-Area-Network. Upgraded workstations, servers, and network topography. Work included inventory, budgeting, purchasing, coordinating vendors, and training.
- Created, developed and sold a billion dollar voucher payment system to New York City. The operational, processing, and programming access controls improved accuracy, reduced fraud, and check processing.

Business Continuity Planning/Disaster Recovery

- Managed, designed, implemented, and maintained clients Business Continuity (BC) and Disaster Recovery (DR) site plans. Coordinate testing of the BC plans and DR "hot" site recovery procedures. Pro-active planning significantly improves incident recovery times.
- Authored and prepared statements of work, business impact analyses, risk assessments, business continuity plan evaluations, and disaster recovery plans for clients. Presented quantitative/qualitative risks including countermeasure solutions to C-level management and shareholders in a clear manner. These recommendations helped define and mitigate risks throughout the client's corporation.
- Developed new disaster recovery managed service offerings, utilizing internal and outsourced delivery resources.
- Community Emergency Response Team (CERT) training in disaster preparedness, fire safety, disaster medical operations, light search and rescue, disaster psychology, and terrorism. Active member in community awareness training.

Information System Specialist, The Cancer Institute of New Jersey
New Brunswick, New Jersey   1995 to 1997
Management/Security
- Planned and developed the LANs/WANs for the newly established Cancer Institute. Coordinated and expanded the connectivity to affiliated hospitals. Created and implemented security processes and access controls within the organization.
- Directed planning, budgeting, acquisitioning, installed, and repaired hardware/software for clinical and non-clinical departments. Ensured hardware and software were in policy compliance with Cancer Institute, affiliated hospitals, and parent university.
- Supervised support team and trained support staff on help desk operations and change control mechanisms.
- Managed educational, research and administrative computing services. Implemented and taught the first enterprise-wide security awareness and training program for the Institute and affiliated hospitals.
- Passed technical audits to obtain certification and accreditation in becoming a Comprehensive Cancer Center designated by the U.S. National Cancer Institute.
- Maintained contracts with outsourced vendors. Negotiated service level agreements including monitoring and reviewing vendor's performance

Engineering, Operations, and Programming
- Designed the first disaster recovery and business continuity manual for the Institute. Wrote business impact analysis report for clinical and non-clinical areas; determined time-critical functions; maximum tolerable downtimes; documented work and presented to department supervisors.
- Planned and implemented the technical patient privacy policy strategies for clinical/non-clinical systems.
- Wrote clinical/non-clinical databases and designed software for specific applications. Created tumor registry database used by Cancer Institute and affiliated hospitals. Wrote operations documentation. Created backup and restoration procedures.
- Assisted in the implementation of a statewide oncology professionals tele-educational and tele-medicine program.
- Technical consultant for affiliated hospitals providing needs and risk analysis of hardware and software systems.
- Diagnosed and repaired computer hardware and software for entire institute and satellite offices.

Director of Management Information Systems, Rosenberg, Druker & Co
Bridgewater, New Jersey   1989 –1995
Management
- Responsible for recommending, installing, and maintaining network for the firm's multiple offices and billable clients.

- Implemented projects for accounting systems, desktop publishing, word processing, database management, spreadsheets, optical scanning, and project management.
- Supervised and planned the department's budget and expansion. Determined the computer policies for the entire firm.
- Wrote Business Continuity Plan for all offices. Sustained hot-site locations during mission critical tax season
- Solved a diverse array of computer problems for the firm and their clients.
- Taught in-house and external Management Advisory Services accredited training programs.

EDUCATION:
B.S., Computer Science, September 1986, Monmouth University, West Long, New Jersey

CERTIFICATION:
Certified Information Systems Security Professional (CISSP)
Information Systems Security Management Professional (ISSMP)
Member of Business Continuity Institute (MBCI)
The Open Group Architecture Framework (TOGAF) Foundation and Certified Architect