Matthew Kaufman | 732 604 0387 | mkaufman1@gmail.com | LinkedIn: linkedin.com/in/matt-k-6113b732/

Executive Summary

Technology executive at the intersection of enterprise risk and business growth with 18 years of experience, combining executive presence with technical credibility to build security governance programs that withstand regulatory scrutiny and align cybersecurity investments with business priorities. Currently Head of Cybersecurity Governance at IDB Bank, directing implementation of cybersecurity strategy. Track record of partnering with cross-functional teams to drive consensus-based decisions to achieve cybersecurity maturity with oversight of a $3M budget.

Core Competencies

Cybersecurity and AI Governance • Regulatory Compliance • Enterprise Risk Assessments • Executive & Board Reporting • Audit & Regulatory Remediation • Incident Response Governance • Tabletop Exercises • Third-Party Risk Management • Vulnerability Management • Application Security • Secure SDLC • DevSecOps • Cloud Security (AWS/Azure) • IAM & Data Protection • Security Metrics & KRIs • Security Policy & Standards

Tools & Platforms: Splunk • CrowdStrike • Qualys • Tenable • ServiceNow • Archer • Checkmarx • SonarQube • AppSpider • Netsparker

Regulatory and Security Frameworks

- FDIC • NYDFS 500 • FFIEC • NIST CSF • CIS Controls • ISO 27001

Work Experience

Israel Discount Bank (IDB Bank) New York New York – June 2022 to Present
Vice President - Head of Cybersecurity Governance (CIO organization)

- Own enterprise wide cybersecurity governance across engineering, risk, and operations enterprise-wide, reporting directly to the CISO; manage a $3M cybersecurity budget and the full-time consultants supporting multiple security engagements.
- Trusted by executive leadership to represent cybersecurity in regulatory examinations from FDIC and DFS.
- Reduced risk reporting timelines by 50% by standardizing the bank’s view of cyber risk by building a suite of dashboards that integrate risk indicators
- Reduced repeat audit findings 100% by overhauling how issue evidence and remediation are tracked and owned.
- Own the cybersecurity issues management program end-to-end through all stages including identification, tracking, remediation planning, and closure — for exercises such as FedLine, SWIFT CSCF, and internal audit findings, managing 15+ open issues at any given time in Archer.
- Partner across vulnerability management, security engineering, IT asset management and Application Security to keep governance embedded in IT processes.
- Lead vendor evaluations (e.g., ZeroFox) for the CISO, evaluating vendor claims against real performance before committing budget.
- Helped shape AI governance control requirements, including CrowdStrike's AI detection and response capabilities, ensuring AI systems are secured from a controls perspective.

Mizuho Americas, New York New York (December 2018 to June 2022)
Vice President (April 2021-June 2022) | Assistant Vice President (December 2018-April 2021)
Information Security Officer – Americas Risk Management (2LOD) & CIO Organization (1LOD)

- Led governance oversight for the enterprise Incident Response program, including tabletop exercises, policy management, and maturity initiatives.
- Built and led the bank's first application security governance program, collaborating with developers on SAST/DAST testing across 100+ applications (Checkmarx, SonarQube, AppSpider, Netsparker).
- Built KRIs and reporting metrics to track application security risk and remediation progress.
- Worked directly with Internal Audit, Compliance, and Risk Management to close remediation items and keep governance controls audit-ready, using Archer as the system of record.
- Rewrote security policies for cloud, acceptable use, and end-user computing. Ran monthly security awareness communications.

BNY Mellon, New York, New York (June 2017- December 2018)
Vice President-Information Security Specialist

- Led and quality-controlled cybersecurity assessments for bank affiliates and third parties using NIST, ISO 27001, and BNY Mellon's Cybersecurity Services Model.
- Identified control gaps and vulnerabilities, partnering with stakeholders as part of the mergers and acquisition process to fix root causes across several boutique banks and affiliate institutions.
- Built cybersecurity maturity dashboards that improved executive visibility on program adoption and risk-based decision-making across business units.

Blue Canopy Group, Arlington, Virginia (September 2014- May 2017)
Security Assessment Technical Lead and Security Subject Matter Expert

- Led 20+ NIST 800-53A security assessments for federal enterprise systems.
- Coordinated vulnerability assessments and penetration testing aligned with OWASP Top 10 using Tenable, Splunk, and SailPoint.
- Developed Windows and macOS security configuration baselines to meet USGCB and FDIC requirements.
- Led secure architecture review and remediation initiatives as a trusted advisor across infrastructure and application environments.

Certifications

CISSP | CGRC | CDPSE | CCSK | GCAD | GCIH

Professional Affiliations

- ISC2 NYC
- ISACA New York Metropolitan Chapter

Education

George Mason University, Fairfax, VA

- M.S. Applied Information Technology, 2013

- B.S. Management, 2008