GARY GOGNA

US Call: 704.451.6101 US Citizen with Public Trust Clearance **E-mail:** gognanyc@gmail.com

Enclosed is my resume for the role of an innovative **Chief Technology Officer (CTO).** As a core CRO – CIO - CISO evangelist, and a hands-on, results oriented Information Technology Management Professional, my true value lies in providing the business enabling risk protection a premiere institution requires, while blending that protection and privacy seamlessly into the business landscape.

As your new CTO for One Park Financial, I am confident to value-add with the following seven attributes:

- **Secure collaboration** among my stakeholders via effective vendor leadership, team work and communication at all risk levels.
- **Create and enable critical asset infrastructure protection** via laser-focus enriching mind & technology for election security effort.
- **Provide a secure business environment**, tailoring it to your work needs: right education, trainings, awareness & enhancements.
- **Reduce enterprise risk** by implementing cutting edge processes to assess, analyze & mitigate cyber risks, threats & vulnerabilities.
- **Operational excellence** through innovative IT Governance Risk management of people, polices, processes & procedures (GRC's).
- **Develop core systems audit defense**: business continuity & disaster recovery (BCP/ DR) capabilities as a strong business enabler.
- **Allow for the maximum modernization** of mission critical asset - infrastructure / operations business systems where possible.

Trained and/ or Certified with:	Cert. Known as	Organization	Passing
Certified Chief Information Security Officer: Info. Security Risk Mgt.	C| CISO	EC-Council	2014
Certified in Risk Info. Systems & Controls: Governance Risk Controls	CRISC	ISACA - IIA	2010
Certified Information Systems Auditor: Audit & Compliance Risk	CISA	ISACA - IIA	2017
Certified Ethical Hacker + Computer Hacking Forensic Investigator	CEH - CHFI	EC-Council	2013
Six Sigma Master Black Belt: Process Re-Engineering/ Improvement	SSMBB	ISI - B	2008
Certified Information Systems Security Professional: Trained Techno dyne	CISSP	ISC2	2008
Certified Information Security Manager - Trained: via ISACA	CISM	ISACA	2009
ISO-IEC Certified Lead Auditor: ISO27001, Trained on 27005,27018,31000	ISO Auditor	ISO / IEC	2018
Certified Internal Auditor: Certified Fraud Examiner CFE, and CAMS	CIA	IIA - Others	2016
Project Management: PMI Certified + Prince 2 Practitioner Accredited	PMP-Prince2	PMI ,OGCUK	2006
New York State Department of Financial Services 23 NYCRR 500 Reg.	NYCRR 500	NY State	2018

FORMAL EDUCATION:

- ✓ **Master's equivalent in Advanced Risk Management (CRMA)** through a PGD Certificate IIM-Bangalore year 2007.
- ✓ **Bachelor's in computer science** - Information security & Risk: University of North Carolina-Charlotte, year 2003.

PROFESSIONAL SYNOPSIS:

- **Master craftsmen** for ISMS, Security Governance, ERM Risk & Compliance, Operational Risk and Fraud Risk; **has managed GRC.**
- **Reported** directly into CEO, CRO, CCO, CAO, CIO, CISO, CTO, CMD and other C-level members for executive board / city council.
- **Dealt with ISO 27001, NIST 800:53, COSO, COBIT, PCI-DSS, EU-GDPR, HIPAA, US Privacy, SOX, ITIL, FISMA, FFIEC, ISAC, Mitre.**
- **Worked with** both external and internal stakeholders (US Govt. as well as Inter-Govt. Intel agencies), where I managed the ISMS/ ISO risk detection & prevention deployments, including new product developments based on AI and Machine Learning.
- **Largest: Team Managed: 5000+ including VMO Ops., impact size: 100 million users, budget size: 248 million with 27+ Directs.**
- **6 time Risk Steering Committee Member for Merger-Acquisition:** Information Security GRC, IRB's, Audits, Risk and Compliance.

I am definitely someone you can reply upon: when it comes to Enterprise Risk, Information Technology based, Infrastructure, Info. Security Governance / IT Risk Compliance Mgt. initiatives**. I can be very handy especially when**: it comes to the strategic ISMS planning and executing all these business risk strategies, working with requisite IT-IS governance, risk, privacy and compliance, relative execution's including any new product mgt. oversights, or relative monitoring work, including Security Incident Management and Response (SIRT), Security Threat and Vulnerability Management (SIEM) , Enterprise Risk Management, Security Administration (ORM); Information Security Education and relative Training awareness. I have worked with right from a BIA, ROI, risk and vulnerability assessments to detection – prevention - due-diligence, to risk mitigation & remediation tech's, operational performance, breach mgt.: recovery, investigations or inter-departmental oversights. These include relevant resource building, financial budgeting, specific publications (if any), corp. communication, PIO and working with inter- Govt. US agencies such as DHS, FBI, FS- ISAC, CIA & other Federal CJIS teams.

WORK EXPERIENCE:

Universal — Jan 2012 - Till Date

Clients: Canara Bank, A HMO, Federal Judiciary and Transit Authority (Consulting): 100 % travels

Role: SVP – Dy. CISO / CTO (Chief IT Risk, Security & Compliance Advisor for the CIO, Exec. Boards Council)

- Reported directly to CISO / CIO, dotted line for Chief Audit & Risk Officer, Chief Legal / Company Secretary for various UCG clients.
  - **Managed a 07 member ISMS & GRC team** consisting of SME's for cyber security, risk, audit, and for maintain core GRC initiatives. This core team maintained the technical disciplines for SOC, info. security incidents, overall risk governance strategies, basic risk assessments, besides the event monitoring & risk threat analysis through SIEM, SOC and Security incident response mechanisms.

- **Liaised on with various teams including enterprise risk architects, specifically over IT web applications, infrastructure, and operations Management teams / process owners to help alignment between security and enterprise architectures.**

- **Worked with Risk and Audit Committee** team members over audit findings to help business processes / technical improvisations.
- **Worked with new implementations** e.g. Office 365, Amazon AWS, Microsoft Azure Cloud Computing, Splunk and Tenable.
- **Worked in conjunction with other outsourced vendor big 4 teams** within the governance and risk workflows to assist with semi-annual audits, third party risks, business continuity, disaster recovery plans and forensic investigations.

- **Provided strategic risk guidance for various IT projects**, including the evaluation & recommendation of technical ITGC controls.
- **Assisted with creation facilitation and supervision / management of SIEM (Security Incident and Event Management),** SOC (Security Operations Center) and **SIRT** (Security Incident Management Response teams) processes and relative event management (addressing / minimization of risks, vulnerabilities and negative finding's) to protect NY, CT, DC City Council's IT assets, including the Data, reputation and various intellectual properties.
  - **Worked with guidelines and frameworks such as NIST 800: SP 30, COSO, COBIT and OCTAVE including ISO 27001 & 27005.**
- **Maintained effective external working relationships with government regulatory agencies**, city council, city departments. Assisted with the creation and overall management of various Risk Mgt. & Information Security awareness training programs.
- **Provided technical direction and oversight** to the delivery of security as a service, while ensuring alignment with organizational goals and objectives including **designing, architecting a centralized SIEM and SIRT program for SOC Compliances.**
- **Worked with senior leaders in the technology infrastructure, privacy, and enterprise risk spaces** to help ensure risk and controls met both business needs and regulatory requirements over Azure and AWS Cloud services (SaaS, IasS and PaaS).
- **Engaged business process owners and managers, including application delivery teams, and the audit heads** to ensure alignment with organization objectives -Acted as central point of contact for all headcount requests prior to CISO approval.
- **Resource management for a dedicated core team** responsible for a wide variety of technology and risk related disciplines.
- **Enhanced ISM operational reality via operational monitoring efforts**: banner logins, sign on acceptable use policies, cyber security awareness training with better risk controls. Other responsibilities included executive board reporting, triage mgt., and investigation of security vulnerabilities that could lead to breach of privacy of all end customers from operational arena.

- A**ssisted the subordinates with Third Party Oversight (TPO) and vendor activity** through coordination with Delivery Managers including process, policy education -governance, budget validations for relevant stake-holders including Finance and Audits.

- **Supervised people, processes and technologies** for making timely, informed decisions (choices) for the Executives via Rapid Risk Response Management. Here. I gained a strong **understanding of cyber kill chains, counter terrorism cyber-intelligence, fraud risk analytics illuminating risk blind spots and actor based threat investigation forensics and chain of evidence, including cyber business intelligence, data collection via investigation and reporting tools** such as **Nmap, Splunk, Encase Forensics and Tenable Vulnerability Scanning System (CVSS).**
- **Assisted few clients internationally** – e.g. Holy Family Hospital & Canara Bank via another consulting venture over the years.
- Took some time off for personal family reasons: sick family members, and including personal health, other family reasons.

TD Bank North Consulting: New York - US & Toronto Canada **Year 2011**

Level: SVP **(Deputy Chief Risk and Compliance Officer for TDAF M&A: including GRC and Info. Sec. Office)**

- Acted as Deputy Chief Compliance Officer in absence of Global Chief Compliance for the bank's M&A operational activities.
- Co-managed a team of 8-10 SVP bank executives over CRM PMO & M&A initiative, advising 150,000 bank professionals worldwide from a regulatory reporting, consumer compliance and bank risk policy perspective.
- Executive dash-boarding of strategic initiatives like ORM, BAU, Cloud Computing, cyber risk, frauds and information security.
- Advised a team of 27 SME VP in compliance risk, regulatory risk and privacy risk initiatives for bank systems and processes
- Program Portfolio Net worth: 2 billion in assets as a firm and 27 million transactions per month.
- Supervised various LOB's over business, technology and vendors risk management from CRM and CISO office perspective.
- This included ensuring identification of significant technology-related M&A risks and the implementation of control processes and techniques to safeguard TD Bank and its customers from internal and external vulnerabilities and threats.
- Managed an implementation of corporate compliance policies, procedures and standards from US Privacy, SCRA, FCRA, Fair Lending, Consumer Compliance, Fraud BPO, IT Security among other LOB perspectives, and provided strategic direction and leadership for relevant TDAF CRM integration work:
  - Helped develop and create new processes, procedures and standards for accomplishing various TDAF work flows.
  - Interfaced with all levels of management to negotiate program level priorities and outcomes.
  - Worked with SME's having thorough knowledge of applicable federal and state regulations (MA, NY, MI, FL) e.g. Mortgage lending reviews, Fair Lending, FCRA, SCRA among others.
  - Reported compliance issues and gaps to senior management including the CRO, board level and the Audit Challenge Committee, prepared presentations to the FRB – NYC and Philly and OCC with respect to bank's Compliance Risk.
  - Responsible for managing company litigation and for overseeing outside counsel in state and federal matters, including corporate, regulatory and loan origination cases.

- Reviewed respond procedures to allegations of unfair and deceptive practices ("UDAP") and complaints related to consumer protection, predatory lending, fraud, and federal requirements.
- Reviewed and revised vendor management operations (VMO): contracts, nondisclosure & confidentiality agreements.
- Responsible for the development, implementation and administration of all aspects of the company's CRM & ISO.
- Worked with other peer organizations over security awareness / training workflows via FS-ISAC, DTCC and SIPC.
- Worked with Consolidated Audit Trail (CAT) system security and other principle obligations as set by SEC Rule 613.
- Assisted with development of policies and procedures to foster a culture of bank-wide security risk & compliance.

Citi Bank NA Consulting: New York City, Chicago & San Francisco– US **Year 2009 - 2010**

Role: Program Director BISO **(PM3 Consultant: Fraud Risk Management Director and BISO Advisory)**

- Managed BAU, ERM policy changes, Fraud strategy analytics, program management, security governance and its adherence.
- Strategy execution and deployment: Actimize Fraud Risk Manager and RCMS (Risk Case Management).
- Budget Portfolio: $30 million with yearly savings of $2.1 million as part of global fraud risk and ISMS deployments ROI.
- Worked with technology and vendors providing support over a broad range of institutional risks and issues, priorities, escalations from execution and risk management, this included Fraud risk and Information Security awareness trainings.
- In cooperation with H.O. Citi NA Cybersecurity Dept., I have assisted in the development and overall maintenance of Fraud Risk and Information Security policies around Citi NA Cybersecurity objectives that would define baseline ISO / ISMS policies
- Assisted business process & steward owners in different business units to establish appropriate security objectives. This included network operational monitoring on a supervision level for maintaining operational reality checks through banner log-in, and systematic checks for insider threats, and real time RBAC (role based access controls) as provisioned.
- Strong supervision with security analysts over CVSS reports for system vulnerability: this included some hot-fixes and/or automated security patch and configuration mgt. along with change mgt. controls for various already deployed platforms and system technologies (Automated the detection and prevention process, worked with Breach Mgt).
- Monitored the BISO process with creating, changing, or removing user access across all systems (employee ingress and egress (intakes and exits)) – this included Password Managers Management adhering with the password requirements.
- Also assured that all appropriate documentation pertaining to the record-keepings of various account creations, deletions, and permissions are correctly maintained and approved. Monthly senior executive management reporting and presentations.
- Oversaw fraud and data privacy related SIRT investigations, escalations and post mortems with specialized units dealing with financial crimes involving fraud analytics and policy owners (over Data at rest, Data at transit and Data In-Out over Cloud Computing Services being rendered for, through Amazon AWS Cloud Computing Services).
- Regular interaction with senior CISO / CTO level among other C-Level leaderships and board of directors.
- Conducted Corporate Information (prevent, detect and respond) Security Awareness and ERM training for initiatives affecting ORM and BAU, operational effectiveness and client experience.
- Involved with cyber analytic, end-point security management, data protection and privacy-risk investigations, SIRT , Red team mgt., fraud prevention and fraud detection cycles, audits and regulatory authorities.
- Vendor management (VMO) and selection experience: 1 on 30 vendors via RFI, RFQ, RFP, RFT.
- Maintained, cultivated, and managed various business relationships among strategic partners.
- Exposure to organized criminal groups who operate in check fraud, internal bank fraud and electronic crimes.
- Maintained meetings on the following: risk logs, issues, problem areas, threats and system vulnerabilities including risk registers and performance measurement – scanning and assessments through software like Nessus Tenable and NMAP.
- Oversaw / Supervised the security program = SOC portfolio, its relative work-strategy and security governance for ISMS.
- Worked with cyber SIRT teams and assisted in retail bank and cyber frauds investigations. Strong exposure to bank fraud detection and prevention systems, mitigation strategies from FDIC and FFIEC examinations and cyber and bank-wide fraud assessments perspective. Managed and performed IS security and audit reviews on a quarterly, annual, and ad-hoc basis. Fostered new control and direction setting resulting in client cost savings.
- Deployed effective information security strategy program, incorporating best practices for a major overhaul on enterprise level data management, re-calibrated security controls via IT security management and governance protocols with SIRT team for Identity and Access Control Management (IAM) through Quest software.
- Assisted in the delivery of a continuously improving end-user educational program to raise cyber security awareness and the understanding of information security and associated security risks.

American Express Consulting & Wachovia Sec. Full time, Scottsdale AZ & St Louis **Year 2008 and 2009**

Role: Head of IT PMO **(VP Consultant: Networks Security IT Risk and PMO: GMS & Global Info. Security Office)**

- Worked as a GMS PMO Program Director, Lead Managerial consultant acting as liaison for business and technologies, saved the firm $250,000 in 90 days via technical health checks on enhanced systems security and risk controls, due-care/due diligence effort master SLAs. Partners included Deloitte and IBM, among others.
- SVP direct report with a dotted line to the CIO on the technology side. Acted as single point of touch – liaison between American Express (AE) Technologies and business side principals. $2 million in savings over five years ROI via a $10 million globally.
- Established baselines for enhanced security standards, data entitlements, ISO policy governance and overall data management and security architecture for strategic work initiatives including GMIS.
- Supervised the "General Merchants Information Strategy (GMIS)" Program. This provided PKI protocol (secured electronic transactions: SET) oversight over three program managers, 11 project managers, among IBM , Deloitte Consultants and other FTEs, consultants, and contractors.
- Moved into NYC – and then economy went into recession – was unemployed for some time between 2008-09 and early 2010.

Bank of America Consulting: New York – Charlotte NC (travel based role) **Year 2006 and 2007**

Role: VP- Sr. Manager **(Sr. Manager for AML KYC Compliance & Online Bill Payments System)**

- Led a strategic enterprise level AML KYC compliance work effort, involving Enterprise Risk Case and Compliance Management system teams from BAC Frauds Prevention teams.
- Closed all major gaps (change management) between 3 major Lines of Business (LOB): Investment Banking (GCIB), Wealth Management (GWIM), and Global Treasury Services with regard to the AML/BSA Act.
- Supervised risk and audit work programs and AML technologies for GRC. I helped integrate Big W with Enterprise Risk Rating System for better compliance and corporate adherence. For example, enhanced reporting and monitoring alerts over all clients, maintaining an Operational Reality protocol.
- Influenced and negotiated with principal partners: stakeholders within the AML Risk/Compliance and GWIM and GCIB structures on quality, timelines of processes, products or services for AML Compliance as KYC multi-generational solution.
- Managed standardization and enhanced due diligence procedure for KYC AML business and technical implementations. Specifically, watch list screening (NESS and STS: real time, on demand, batch customer filtering, list integrations, new customer verifications), customer due diligence (KYC: know your customer solution), and Suspicious Activity Monitoring (SARs), CIP (Customer Identification Program), identity verification, risk ratings technical platforms, negative news from credit agency bureaus, certification tracking processes, enterprise-wide training program on Anti Money Laundering, BSA, Patriot Act and fraud prevention.
- Another $ 10 million online banking ecommerce initiative (Bill Integrations Online Payments) Impact: 90 million users, Team: 100+

Capital One Consulting: Richmond VA & London- England **Year 2004 and 2005**

Role: Head of PMO **(T6: Sr. Director: Governance, Risk Audits, and Compliance over IT, Data Risk & Privacy Mgt.)**

- Ran, governed and managed almost all aspects of two NCR Teradata "Running the Engine" and "NCR Teradata - Best Practices" enterprise-wide (EI) programs for Data Management Services Domain through Technology Services and Solutions (TSS) team.
- Managed a Portfolio of 37+ projects; domains included Data Risk Management and Information Security based workflows – IAM, Least privileges, Single Sign On, RBAC, Cyber Maturity Programs, Corp. Risk and Controls, Opex. Business Excellence, ETL, Data Cleansing, Data Governance, Security Risk, other Reporting and Analytics.
- Managed 90% transactional and Master Data Management (MDM), including vendor risk Mgt for NCR Teradata, InfoSys, TCS & IBM.
- 20 direct reports at one time and over 500+ team member teams in the portfolio across various parts of the organization.
- 190+ application legacy systems consolidated into running the engine "Single truth – Common View" platform as a IT PMO Head.
- Duties included business operations and technical governance, role based access control: corporate security, capacity management, new product development and relevant rollout coordination, release management, governance, resource prioritization, ERP (SAS), budget management, risk, business objectives / scope management.
- Project reporting tools included basic SQL, Plainview – BEN - Clarity PPM, MS-Project, Project One, Prince 2 Practitioner level = was awarded Outstanding Performer (PM3 level or higher) – Capital One, February 2005.

Note: S.E. Consulting stands for Self Employed based Consulting ventures. Secondly, I did take a few /some time off(s) for personal family reasons between Oct 2004 – till date. I'm a living person and life circumstances / things do happen in life.

FT Employment at: FIRST UNION – WACHOVIA BANK: CHARLOTTE NC **Oct 2000 – Oct 2004**

Role: Analyst / Manager **(Global Treasury Services: Lockbox, ERM – ORM and Corp. Risk)**

- Managed and supported medium to large complex projects / program related with various work streams, dealing with multiple lines of businesses like OTE & GTS. Key areas were retail operations, small consumer and commercial divisions like cash and transactional processing, and ACH. New product launches: SSO, RBAC, AML Regulatory Compliance, and ERM. Managed vendor relationships with Deloitte, KPMG, PWC, IBM, and Cognizant. Member to merger & acquisition governance team for investment review boards Wachovia.
- Supported operational risk and big transactional data risk management workflows for Corp. banking functions, ERM & Capital Markets.
- Improved and contributed to processes workflows for corporate level Information security risks and controls around RBAC (Role Based Access Control) initiative, IAM (Identity Access Management) and Single Sign On - SSO deployment (2 yr. work effort) with IBM Tivoli.

System Tools and Other Work Exposures (at the Management Level):

- ISO / Data Mgt. Tools: NCR, Teradata, Hadoop, EnCase, Actimize, Splunk, Tripwire Enterprise, VMware, Kali, Nessus Nmap, Tenable, Quest.
- Familiarity with ISMS Policy Frameworks: ISO27001/05/38500, ITGC, SSAE-18, HIPAA, Hi-Trust, COSO, COBIT, OCTAVE, FISMA, NIST 800:53.
- Has worked with new Technology/ policy based on: Identity Thefts, IAM, RSA Enterprise, PCI-DSS, Office 365, Azure & AWS Cloud Computing's.
- Regulations Familiarity: SOX, SSAE 18, HIPAA, PCI-DSS, BSA – AML - KYC, US Patriot Act, FCPA, OCC, FISMA, FDIC, FFEIC, GLBA, CCIPL, EU-GDPR.
- Methodologies - Process Framework: PMI, SDM, SDLC, Agile Scrum, ITIL, PMO Best Practices, Prince 2 and Six Sigma DMAIC, Plan Do Check Act.
- Microsoft Office applications: (MS Word, Excel, PowerPoint, Outlook, Access, MS Project & Visio), SharePoint, PPM & time entry.

I will look forward to the in-person interview call. Thank you for giving me your time and considering my candidacy today.