Executive Director - Information Security, Cybersecurity, Technology Regulations, Enterprise Risk Management, BHC, Policy Program, IT Audit & IT Governance (Full-time) Executive Director - Information Security, Cybersecurity, Technology Regulations, Enterprise Risk Management, BHC, Policy Program, IT Audit & IT Governance (Full-time) Executive Director - Information Security, Risk Management, Cybersecurity, Regulatory Program, Policy & Standards, IT Governance & GRC New York, NY Skills: Executive Management. Senior Leader in Information Security, Cybersecurity, Enterprise-wide IT Risk Management (IT ERM), Regulatory Readiness across global Technology, Policy and Standards, IHC / BHC Program Management, Governance, Risk and Compliance (GRC), IT Risk Strategy and Assessment, IT Governance, Data Privacy (GDPR/GLBA/CCPA), Data Protection, IT Compliance, Data Classification, IT Assurance, Third Party Vendor Security Management, Disaster Recovery and IT Audit/SOX. Authorized to work in the US for any employer Work Experience Executive Director - Information Security, Cybersecurity, Technology Regulations, Enterprise Risk Management, BHC, Policy Program, IT Audit & IT Governance (Full-time) Goldman Sachs - New York, NY January 2018 to Present Information Security, Cybersecurity, Regulatory (IT) Regulations for Technology, Enterprise Risk Management (ERM), Policy & Standards Author, Data Privacy, Governance, Risk & (IT) Compliance (GRC), Risk Assessment, Cloud, Data Security, IT Security, Data Classification, Data Protection, Data Risk Management (DRM), SOX & IT Audit Management, Third Party Security Management, Vendor & Supplier Risk Management, Bank Holding Company (BHC), Incident Response & Training & Awareness. Lead and manage several Technology Risk programs, including operational delivery, execution and support. Cybersecurity / GRC SME (Full-time) ManTech International Corporation - Jersey City, NJ December 2017 to January 2018 Provided oversight & roadmap guidance on the implementation & rollout of new GRC solution. Lead IHC Security Advisor- Information Security, Cybersecurity, IT Risk Management, IT Regulatory, Policy & IHC Program Management (Consultant) BNP Paribas USA Inc., - Jersey City, NJ December 2015 to July 2017 Reported to the Chief Information Security Officer (CISO). Built out new Intermediate Holding Company (IHC) Information Security Program (ISP) per Dodd-Frank Act. Provided risk management, information security, regulatory guidance, including cybersecurity in the newly created IHC program with day to day oversight, leadership & authorship. Designed the BNP IHC information security/cybersecurity strategy, evaluated & analyzed regulatory requirements into viable project plans, solutions & implemented programs and shared regulatory insight and pertinent guidance with Senior Mngt and IHC peers. Wrote all IHC Information Security policies, of which two policies were approved by the IHC Board and the other polices by the Operational Risk Committee (ORC) to ensure accountability and implementation by Information Security & IT. Enhanced BNP Paribas USA Inc., Information Security IHC Program per the 2010 Dodd Frank Act (DFA) requirement for Foreign Bank Owned (FBO). Gary joined BNPP in December, 2015 to deliver the go-live, July 1, 2016 functional program per DFA into having an active, operational IHC information security program and maintained and incrementally improved the overall program by providing cybersecurity and technical engineering strategies, IHC program leadership, policy clarity and info security/cyber/risk/grc SME expertise, for day to day decisions, aiding project leadership, tracking new, known, bank owned and inherited legacy risks and all active or late exceptions /solutions, providing metrics and reports for timing, informative and/or required action status, addressing ongoing challenges in info security, cybersecurity, third party security with vendors, application security risk assessment evidence and question/answer improvements, production operations security, network security, regulatory exams and IT audit areas, and ensuring remediation mechanisms on behalf of the IHC several Business. Kept the risk appetite gauge indicators within acceptable ranges, and advised/escalated upwards when signals dictated otherwise. Experience/Skills: Information Security, Cybersecurity, Enterprise Risk Management (ERM), Regulatory Readiness, Policy/Standards, (IHC) Program Management, IT Governance, Cyber risk, Data/ IT Security, IT Compliance, Reporting & Metrics, IT Assurance, Privacy, Data Protection, Data Classification, Third Party Security Management, Governance Risk & Compliance (GRC), Disaster Recovery/Resilience & IT Audit. Managed the IHC's Information Security with Cybersecurity program with Risk Management, GRC, IT Compliance, Regulatory Readiness, IT Audit Facilitation, Reporting and Training/Awareness Guidance including: Advised Board, Committe's, Executive & Senior Management, Staff & Consultants on IHC Information Security matters. Received Confidential Supervisory Information (CSI) clearance as an IHC Information Security & Cybersecurity lead Consultant, in meeting the two primary Regulators, FRB NY and NYDFS. Implemented incremental IHC program infosec/risk/cyber/grc/regulatory/audit enhancements. Lead Information Security/Cybersecurity training with data, privacy & physical security awareness practices, communications, habits and ideas for users. Designed and wrote the revised IHC 2017 Information and Cybersecurity Strategy content for the NYDFS Cybersecurity requirement due by March 1, 2017 regulation, along with IHC CISO's input & feedback for IHC Board's for approval and adoption to be compliant. Ensured regulatory compliance with appropriate risk metrics feeding the operational risk appetite and tolerance levels with the Business and IT. Wrote and authored six new Information Security policies and provided commentary/feedback on many other related IHC risk and related policies. Reviewed multiple different policies and standards at the Operating Entities (OE) level to ensure coverage across IHC InfoSec ecosphere. Collaborated with Executive Management on annual, quarterly & ad-hoc Information Security and related Cybersecurity reports and metrics, including the regulators (U.S. and EU) & internal audit/Inspector Generale. Organized and reported on successes and risks for the Board and several Risk and Policy Committees and in the InfoSec/CyberSec Forums. Managed security workload/projects/plans/requirements across multiple Information Security, Cyber, Audit and Regulatory units. Created 1-stop InfoSec IHC shopping and coordination program (excluding reports & metrics, handled by another dedicated IHC senior security peer) with the 3 Operating Entities (OE's) Mngt & Staff with their operational specifics. Created, fostered and actively maintained 1st, 2nd & 3rd Lines of Defense (LoD) Business, Management, Security, Legal, Regulatory, Compliance, IT, HR and BCM relationships and dialogue in the IHC InfoSec program. Evaluated inherent risks, mitigating controls, understanding identified gaps and potential remediation(s), communicating with action plan owners and tracking to completion. Worked on and agreed to acceptable (residual) risk levels and reporting of issues through escalation processes when triggers approached/broken, as required, or when thresholds breached. Monitored and tracked application and infrastructure related and interconnected risks/gaps, action plans and on-point solutions with deliverable dates. Evaluated security/cyber risks from assorted risk assessments within data, application, infrastructure, software, hardware and/or services/platforms (hosted internally and/or externally by 3rd Party or Cloud Provider(s) to ensure required and satisfactory security controls over sensitive data. Evolved to version 1.1 from the July 1, 2016 v1.0 ISMS overall Program. Required better security with data protection programs, policies and tool capabilities for the intrinsically more important and valued business and customer data through classification initiatives, on-going metadata tagging and DLP efforts. Ensured IHC data classification policy was reflected in the assortment of assessment questionnaires/processes and, in the records management. Operated Business-As-Usual (BAU) information security program with cybersecurity and IT related operations with efficiency as technology, personnel, usage, risk issues and maturity to incrementally improve over time to raise the standards bar to be able to detect more granular anomalies, threats, vulnerabilities and patching in the work environment. Checked internal corporate shared services versus 3rd party vendors & suppliers and implemented more stringent information security risk management practices to our sensitive data per requirements. Worked with the procurement and infosec teams on those engagements. Provided and reported to Management, Audit & Regulatory entities per new guidance for the IHC and its operating entities, when required, in timely manner. Re-organized Information Security Program (ISP) per CISO's guidance Developed & enhanced information security and cybsersecurity with IT control frameworks to include; regulatory mapping to FRB, FFIEC, OCC, FDIC, SEC, FINRA, DFS, CTFC, via ISO 27001, NIST, COBIT, EU Data Privacy & Cybersecurity requirements Designed and fulfilled IHC requirements through strategy and policies with cybersecurity and information security processes tied in with IT Risk Assurance & IT Governance oversight processes and directives Facilitated and coordinated with Executive Management on regulatory exam requests & relevant internal IT audit scope letters & final responses Utilized a mixture of several key frameworks to create and evolve the IHC InfoSec Program including; ISO2700x, ISO31000, ISO38500, CoBIT, and the NIST Cyber Security Framework (CSF) etc., Documented, assessed, edited and evaluated policies, processes, plans & Standard Operating Procedures (SOPs) to support the Banks regulatory requirements per Federal Reserve Bank (FRB NY) via FFIEC IT Booklets and supported by NIST's 800/1800 technical documentation guidance   Operated in Three Lines of Defense FRB model, where Information Security partnered with the Business in the 1st line of Defense as 1.5   Reviewed ongoing and new policy requirements, adjustments and feedback to enhance the next rounds of versioning and maintained good information security policies, standards and procedures on an annual check when required by the regulatory laws and/or from internal management timetable changes   Translated metrics into operational risk and security measurements for reporting and being in-sync on enterprise-wide appetite terms for operational risk consistency assurance & accurate program measurement   Delivered information security, cyber security and risk reporting for the IHC on behalf of the 3 OE's and across the Combined U.S. Operations (CUSO) entities, when applicable   Evaluated Third Party Vendor programs, services, providers, suppliers and 4th party and onward sub-contracted relationships, on issues and Service Level Agreement (SLAs) with approved third party service providers, including the subsidiaries, corporate, parent bank (Paris HQ) and related 3rd party vendors, suppliers and sub-contractors   Wrote and built the existing security Target Operating Model (TOM).   Assisted the IHC CISO in the development of the revised 2017 TOM as the IHC U.S. operational program's maturity evolved with the advent of new personnel and skills sets   Oversaw Governance, Risk and Compliance (GRC) risk tracking of security and third party activities with metrics and reports to Management   Developed the Information Security Quality Assurance and Testing in the IHC InfoSec program with the 3 operating entity CISO's and teams (OE's)   Assessed and evaluated training and awareness efforts in coordination with the trainers for year over year improvements on required annual training initiatives to enhance worker recognition for cybersecurity threats when in the workplace, and while at home to develop inquisitive habits.   Reinforced physical security practices such as; tailgating issues, missing or hidden work badges, reporting of issues, locking drawers, securing desktops/laptop and other building security basic concepts   Skills: Information Security, Cybersecurity, Enterprise Risk Management, Regulatory Readiness (FRB/OCC/SEC/FDIC/EU etc.,), Governance, Risk & Compliance (GRC), Policy & Standards, IT Compliance, Risk Assessment, Data Privacy (Clients /

customers / consumers with GLBA & GDPR), Data Classification, Data Protection, IT Audit Facilitation, IT General & Key Controls, Strategy, IHC Program Management, Outsourcing, Third Party Security Management (TPSM), Security Frameworks (COSO, CoBIT, ISO27001, NIST RMF & CSF, ISO31000, ISO38500, ISO22301, ISO25999, ISO15489), Cloud, Big Data, Mobile, Vulnerability Management, Threat Intelligence, Business Continuity Management (BCM), Disaster Recovery (DR), Change Management, Patch Management, Security Incident Response Management (CERT, CSIRT, SIRT, CIRT & SIRM), Training & Awareness, Outsourcing and Security for Vendor / Supplier Management. Senior IT Risk & Security Leader (Full-time) - Information Security/ IT Risk/Cyber/Policy/Controls/3rd Party GE Capital - Norwalk, CT October 2010 to December 2015 Norwalk, Connecticut Senior IT Risk Manager - Risk Management, Information Security, GRC, IT Compliance, Cybersecurity, Regulatory and IT Audit/SOX Facilitation. Enterprise Risk Management (ERM), IT Compliance, Information Security, Governance Risk & Compliance (GRC), Regulatory Readiness, IT Audit, SOX, Policy & Standards, Third Party Security Vendor Management, Data Privacy, IT Governance & Disaster Recovery Implemented (IT) Risk, Information Security, Cyber security, IT Audit & IT Governance programs with ISO, COSO, CoBIT (4.1 + 5.0), NIST frameworks and policies/standards to support company & industry mandates Operated in the Three Lines of Defense model & focused on 2nd line of Defense strategy (Ops Risk & IT) Managed program, cybersecurity risks & designed mitigating plan strategies where gaps require solutions Provided subject matter expertise for regulatory requirements within IT with Legal Counsel & Compliance Operational oversight of Technology risks for any non-compliance to policies, projects, audits, information security issues, DR, records and change management exceptions/exemption requests Improved technology audit results and outcomes in to ensure satisfactory reports and effective solutions for NIST and CoBIT controls and processes implemented in the programs and being compliant in IT. Lead and enhanced the annual risk assessment program with in-depth questions/answers, process reviews, gap remediation and closure, project plan targets & policy changes across the infrastructure, middleware and application, inside and externally with trusted 3rd party providers, vendors and 4th party partners Assessed information security strategy initiatives and assessments when sourcing, third party providers, suppliers and vendor management to ensure correct data protection and global consistency for on premise and off-site premises housing the firm's information.   Utilized new technologies across platforms, projects and company/customer business data directives with SMEs in cloud models, proper use of social media & monitoring, mobile & big data (BI-data lake) initiatives   Designed and prepared the Business and Technology for internal & external audits as well as U.S., America's and European external examiners with the (6) six phases of a Regulatory & Audit program throughout.   Executed regulatory mandates, policies, standards and frameworks suited for Business and Technology (CIO/CISO) to meet new & current regulatory requirements per the FRBNY (FFIEC), OCC, SEC, GLBA, FDIC, FINRA, NYSBD, COSO, CoBIT, HIPAA, PCI-DSS, NIST, BITS & overseas partner regulators/auditors   Managed internal audit findings across identified gaps with successful plans, coordination & tracking to closure   Documented (IT) risks and policy remediation projects to timely mitigation in continuous dashboard monitoring   Worked with senior Leadership to balance changing priorities quarter to quarter & capacity to address/fund plans   Monitored stakeholder(s) corrective actions to address gaps and managing unresolved and/or legacy issues   Took actions on GRC, InfoSec, PCI, privacy, key controls, IT audit & SOX issues/projects for several GE CIO's   Lead BU stakeholders when new policy/standard changes were communicated, supported, monitored & enforced   Consulted with Legal and Compliance SMEs regularly for new (FRB) regulatory requirements such as living wills and IT dissolution/separation plans for the Businesses, IT assets, applications and data flow dependencies   Reviewed IT policies, standards, procedures, processes, SOPs and IT control related risks to ensure appropriate information security/GRC requirements and compliance thresholds were monitored, escalated &reported/ tracked Management Consultant - Information Security My Company (Consulting) - Secaucus, NJ June 2009 to September 2010 Information Security, Risk Management, IT Governance, IT Compliance, GRC, Business Continuity, Disaster Recovery, SOX/ IT Audit, Intrusion Detection, Records Management, Program Management & Privacy Consultant/Contractor - Information Security ADP - Roseland, NJ April 2010 to May 2010 Risk Management, Information Security & Disaster Recovery

Performed risk assessment for top 20 highest revenue business applications in U.S., Europe, Australia & Asia Designed risk questionnaire for application owners, support teams to address security, risk and audit issues Interviewed, documented & prioritized risks for the business, application owners, developers & ADP information security team. 2nd phase of this project did not commence as ADP CISO decided to perform the review in-house Consultant/Contractor - Information Security Information Security & Risk Management - Brooklyn, NY October 2009 to February 2010 Information Security, Risk Management, Audit-SOX, Compliance, Business Continuity, Disaster Recovery & Records Management Developed and built new information security program fulfilling firm's (2010 pre-IPO commitment that did not materialize until 2014 IPO) for strategic IT objectives Wrote 66% of new information security policies and standards to be ratified and approved by Executive Management for distribution pre-IPO in 2010 Reviewed remaining 33% of existing policies for consistency and updated select team procedures in IT Appraised IT procedures and security controls to ensure access to data, applications and systems is granted by authorized managers, whether for business and/or technical and in line with stated job function and risk level Documented all IT security controls to achieve several security objectives (segregation of duties, four-eye principle, logging anomalies, minimal access rights, need to know, confidentiality, data center, etc.) Conducted risk reviews of data security, GRC, disaster recovery, security, human resources, privacy, vendor and third party relationships and services Identified, evaluated and implemented enhanced information security, PCI and IT controls in the development, testing and implementation to production SDLC phases Ensured compliance with risk, data classification, privacy, confidentiality, data protection, integrity and availability of the firm and clients data Critiqued business continuity and disaster recovery plans while assessing vulnerability process Tested SDLC/PDLC processes to assess adherence to current policies and procedures Monitored change management, third party, vendor outsourcing and SOX processes being assessed by EY Provided information security training awareness and tools for IT Management, staff & approved third parties Evaluated IT risks with detailed security surveys, observations, interviews & documented recommendations Drafted new security incident guideline per 2009 revised Employee Handbook and IT Security policies Coordinated with IT infrastructure for threat assessments to respond & utilize CSIRT process/procedures Introduced FFIEC, SEC, SOX, PCI and CoBIT technology frameworks and questionnaires to the business Corporate Information Security Officer (CISO) (Full-time) The Port Authority of NY & NJ - New York, NY April 2009 to May 2009 Information Security, Risk Management, IT Audit/SOX, Records Management, Data Privacy & Disaster Recovery Worked with four business department heads to formulate a new risk (FISMA) plan for information security practices, policies, procedures and projects across the organization & in the physical facilities in NY and NJ Reviewed IT Security policies, tools and training Categorized the agency's privacy policies and procedures regarding the Freedom of Information Act in NYS Discussed sensitive inquiries with lead Privacy Officer before releasing information in the request process Vice President - Chief Information Security Officer (CISO) of Americas (Full-time) Dresdner Kleinwort, formerly owned by Allianz Insurance - New York, NY 2007 to 2009 Information Security, Risk Management, IT Compliance, GRC, Regulatory Readiness, Operational Risk, SOX/ IT Audit, Disaster Recovery, Privacy & IT Governance Oversight: Led and managed Information Security operations, IT Governance, regulatory, IT Audit/SOX issues in Americas Ensured compliance with global information security standards, regulatory and established frameworks; ISO:27001, COBIT, NIST, COSO, FRB, FFIEC, SEC, OCC, FINRA, GLBA, HIPAA, PCI-DSS, BITS & ITIL Implemented global CISO & CIO program with enterprise and local country projects and enhancements Primary lead for annual risk assessment process for Americas Business Unit Dealt with all IT exception issues with the Americas Head of Operational Risk and team Adhered to GRC framework to support IT security, controls and data protection efforts Managed regulatory (IT) requirements conforming to information security & records retention requirements Compliance in the stricter privacy countries where business conducted and if HQ required help, it was given Emergency Change Management approver for all IT operations in the Americas Reported to global CISO, CIO, Operational Risk and Compliance department Heads for program/projects Published and maintained IT risk acceptances in Americas for global Board of Directors to approve or reject Assessed risks and developed remediation plans with actionable results Provided threat analysis for application code and approved security solutions for sanctioned IT projects Assistant Vice President - IT Risk, Business Information Security Officer (Full-time) Citigroup - New York, NY 2004 to 2007 BISO) and IT Controls Officer in Global Engineering Information Security, Risk Management, Data Privacy, IT Audit/SOX, GRC, IT Compliance & Disaster Recovery Program Manager (Consultant) - Information Security Horizon Blue Cross Blue Shield of New Jersey - Newark, NJ 2004 to 2004 Information Security, Program Management, GRC, Incident Management, Intrusion Detection and Intrusion Prevention, IT Audit, Regulatory Readiness, Disaster Recovery, Data Privacy & IT Oversight Manager - Information Security, Risk Management, IPS/IDS & IT Assurance (Full-time) KPMG - Sydney and Melbourne - Melbourne VIC 2003 to 2004 Information Security, Risk Management, SOX/ IT Audit, IT Compliance, GRC, Regulatory Readiness, Disaster Recovery, Intrusion Detection and Intrusion Prevention, Change Management, Data Privacy & IT Governance Manager - Network Information Security Officer (NISO) (Full-time) Prudential - New York, NY 1998 to 2002 Information Security, Intrusion Detection and Intrusion Prevention, GRC, Identity Management, SOX/ IT Audit, IT Compliance, Privacy & Disaster Recovery Senior Consultant (Full-Time) - Enterprise Risk Services, Network & Systems Quality Deloitte and Touche - New York, NY 1997 to 1998 Information Security, Risk Management, SOX Audit, Intrusion Detection, IT Assurance, GRC, IT Compliance, Disaster Recovery, Privacy & IT Governance Assistant Office Manager and Senior IT Systems Analyst (Full-Time) U.S. Trust Company - Stamford, CT 1993 to 1997 Information Security, IT Audit, Disaster Recovery, Video Conferencing, Events Management and Server Room IT Support Education Bachelor of Science in Marketing Le Moyne College - Syracuse, NY 1989 to 1993 Skills Information Security (10+ years), Risk Management (10+ years), IT Management (10+ years), IT Governance (10+ years), IT Compliance (10+ years), Risk Assessment (10+ years), Data Privacy (10+ years), Cybersecurity (10+ years), Program Management (10+ years), Risk Analysis (10+ years), Regulatory Compliance (10+ years), Frameworks (10+ years), GLBA (10+ years), GDPR (2 years), IT Audit (10+ years), Policy Development (10+ years), It Security Links https://www.linkedin.com/in/gary-murphy-4a924a Groups ISACA 2007 to Present Children's Aid

Society September 1998 to Present Volunteer with Children ages 5-12 Interview, Resume and Cover letter assistance for highschool young adults

Name: Devin Beasley

Email: robinsonstephanie@example.org

Phone: 738.605.0538