Director Director Director - Afrin Technologies, LLC Laurel, MD With my 29 years of experience in managing information technology (IT), databases, IT security, internal & external security audit, IT risks, cybersecurity, privacy, regulatory compliance; a doctorate degree in management (e-commerce, cybersecurity, and privacy); 14 certificates; and teaching at USA universities for 15 years, I am now looking for a management or subject matter expert (SME) job in IT, database management, cybersecurity, privacy, IT risk management, policy & procedures, critical infrastructure protection (CIP), identity & access management (IAM), incident response, continuity of operation (COOP), active directory, security audit, assessment & authorization (A&A), IV&V, business development, education, training & regulatory compliance. I am a SME in information technology (IT), information security (IS), information assurance (IA), operational technology (OT), database management, GDPR, data security, data privacy, PII, PHI, identity theft prevention, cybersecurity, cryptography, public key infrastructure (PKI), digital signature, single sign-on; ISO 27000 series, FIPS standard, PCI DSS & NIST guidelines, FISMA, HIPAA; contingency plan & drills; president executive orders; OMB circulars & memorandums; cloud security; internal & external audit, CSAM, ATO; awareness & training; risk assessment & risk management; global acts, laws, regulations, policies, procedures, and industry best practices. I was a faculty in the Cybersecurity Department of University of Maryland (UMUC) for 15 years. I have worked on security architecture, IV&V, gap analysis; NIST, CSAM, ATO, SIEM, SOC, NOC, VPN, DMZ, firewall, red team, pre-sale, post-sale, CRM, agile, and secure software development life cycle (SSDLC). I have worked on risk management framework for a bank and digital forensic, imaging, e-Discovery, chain-of-custody, reporting to court for a state organization. I am an expert in cryptocurrency, blockchain, malware protection, e-Governance, and HR; was responsible for organizational vision and strategy at different organizations; developed security documents (SSC, SAR, CP, DRP, COOP, CMP, PTA, ISSP, etc.); conducted ST&E & CP testing; created POA&M and have completed the ATO process of 14 certification & accreditation (C&A) projects for the U.S. Federal Agencies (DHS, USDA, HHS, DOC, DOJ, DOI, US Mint, OPM, FAA, ATF, NOAA), U.S. State Governments (Maryland & Hawaii), and different corporations. Recently, I have served as the head of cybersecurity, privacy, IT risk

management and regulatory compliance at Trump Taj Mahal Casino & Hotel. I was an architect in security vision & strategy, policies & procedures, identity theft, SOC, and PCI DSS implementations. I was a member of the Management Audit Compliance Committee of the Trump Taj Mahal Casino & Hotel and official liaison with the Casino Control Commission & Division of Gaming Enforcement of New Jersey. I have long experience in ISO 26262; Automotive Security & Safety; Internet of Things (IoT) & Network of Things (NoT) security; selecting, implementing, evaluating, continuous monitoring & governing information security controls (NIST-SP-800-30/34/37/39/53/53a/122/137/161); asset protection, pre-sales, post-sales; customer relationship management; identity & access management; designing, developing, operating & managing information systems; vulnerability scanning, incident response (IR), disaster recovery, continuity of operation, backup & recovery, business impact assessment (BIA), defense-in-depth, defense-in-breadth & business development. Work Experience Director Afrin Technologies, LLC - Silver Spring, MD April 2016 to Present IT, Cybersecurity, Privacy, Audit, Risk Management and Regulatory Compliance) Responsibilities: Directing & managing security strategy, database, cybersecurity, privacy, policy & procedure, security audit, incident, impact assessment, e-Commerce, e-Governance, operational technology, and active directory. Responsible for data privacy, accuracy and reliability; consent, lawful collection and obligation; data integration, data sharing & communications, data governess, and human resources (HR); confidentiality, integrity and availability (CIA); privacy threshold analysis (PTA), personally identifiable information (PII), protected health information (PHI), and data minimization; data protection (by design & by default through embedding safeguards in the early phase of the life cycle); privacy impact assessment (PIA), awareness & training, disciplined execution, dispute resolution, security operation center (SOC), GDPR (General Data Protection Regulation), Payment Services Directives 2 (PSD2), implementing cybersecurity & risk management framework (RMF), and regulatory compliance (cybersecurity, privacy, risk, GDPR). Working on PCI DSS (Payment Card Industry Data Security Standard), cryptocurrency, and blockchain security; ISO 26262 & automotive security; Internet of Things (IoT), web security, cloud security, internal & external audit (SOX & FISMA), independent verification &

validation (IV&V), gap analysis, security testing & evaluation (ST&E), plan of action & milestones (POA&M), authority to operate (ATO), certification & accreditation (C&A), assessment & authorization (A&A), risk assessment & risk management, and Security Operation Center (SOC). Protecting digital assets & corporate resources. Ensuring confidentiality, integrity, and availability (CIA). Leading projects on agile and secure software development life cycle (SSDLC). Working on pre-sales & post-sales services, revenue & market share enhancement, customer relationship management (CRM), critical infrastructure protection (CIP), and IT business development (BD). Provided consulting services to a national Information Communication & Technology (ICT) Agency in digital forensics; policies & procedures; identity & access management (IAM); cryptography, public key infrastructure (PKI), digital signature, multi factor authentication, and single-sign-on (SSO); contingency plan (CP), disaster recovery (DR), continuity of operation (COOP), exercises, incident response, and business impact assessment (BIA); vulnerability & threat analysis, cyber risk, cyber-attack, cybercrime, cyber warfare, cybersecurity, cloud security, secure communication, and risk assessment; digital imaging (EnCase, FTK, Tableau); e-Discovery, chain-of-custody, legal documentation & court presentation, and IT risk management. Director Trump Taj Mahal Casio & Hotel - Atlantic City, NJ August 2015 to April 2016 Risk Management, Privacy & Protection, Cybersecurity, Audit, and Compliance) Responsibilities: Official liaison with the Casino Control Commission (CCC) and Division of Gaming Enforcement (DGE) of the State of New Jersey. Member of the Taj Mahal Management Audit Committee. Was responsible for the cybersecurity, privacy, risk management, internal & external audit, digital forensics, regulatory compliance. Safeguarded the personally identifiable information (PII) & protected health information (PHI). Constantly interacted with SOC & NOC to ensure the confidentiality, integrity and availability of the information & information systems. Developed PCI DSS implementation guidelines; strategies, standards, policy, and procedures on information security, GDPR, data management, data privacy & protection, PIA, rules of behavior, and training contents on security & privacy. Developed system security plan (SSP), configuration management plan, risk assessment plan, change management plan, vulnerability scanning plan, penetration testing plan, contingency plan (CP), emergency

evacuation plan, incident response (IR) plan, disaster recovery (DR) plan, and continuity of operation plan (COOP). Conducted CP & IR test and exercises, privacy threshold analysis, privacy impact assessment, identity & access management (IAM), incident response, and business impact assessment. Implemented privacy on casino data, change control board, agile, and secure software development life cycle (SSDLC). Managed, monitored, and inspected to ensure regulatory compliance to the Privacy Act, HIPAA, HITECH, GDPR, FedRAMP etc. in recruiting, training, medical & family leave, player database, and jackpot distribution in Casino Cages. Implemented & ensured cloud security, risk assessment, multi factor authentication, single sign on, customer interaction, IV&V, gap analysis, security testing & evaluation, plan of action & milestones, assessment & authorization and certification & accreditation of the Trump Taj Mahal Enterprise Information System, and Surveillance System. Associate Professor/Course Chair (Cybersecurity and Computer Technology Department) University of Maryland - Adelphi, MD August 2000 to November 2015 3501 University Blvd. East, Adelphi, MD 20783, USA Duration: 08/2000 to 11/2015 Role: Associate Professor/Course Chair (Cybersecurity and Computer Technology Department) Responsibilities: Served as a Course Chair for three (3) years and supervised 12 faculty members. Taught classes in information technology (IT), information security (IS), risk management, cybersecurity, data privacy & data protection, identity theft prevention, certified information systems security professional (CISSP), Network+, enterprise security architecture, application & telecommunication security, incident response (IR), disaster recovery (DR), continuity of operations (COOP), and critical infrastructure protection (CIP) as Instructor, Assistant Professor, and Associate Professor. Guided student's projects in database management, secure software development life cycle (SSDLC), security architecture, cyberspace, cyber ethics, cyber threat, cyber vandalism, cyber weaponry, cyberwarfare, cyber espionage, cyberattack, cybercrime, cyber defense, cybersecurity, privacy, e-Authentication, personally identifiable information (PII), privacy impact assessment (PIA), cloud security, contingency planning (CP), disaster recovery (DR), continuity of operation (COOP) and their exercise & drills; multi factor authentication, identity & access management, single-sign-on, secure access control, public key infrastructure, digital signature, IP, IPsec, DNS, VPN, DMZ,

intrusion detection & prevention, ethical hacking, penetration testing; threat & threat agent; vulnerability scanning/analyzing/reporting; trusted communication & networking; KRI, security categorization, configuration management, system security plan; change control management, business impact analysis, security controls, internal & external audits, independent verification & validation (IV&V), gap analysis, security testing & evaluation, plan of action & milestones (POA&M), assessment & authorization (A&A), certification & accreditation (C&A), continuous monitoring, patch management, hardening, defense-in-depth; cryptography, hashing; confidentiality, integrity & availability; incident response, digital forensic, legal evidence, chain-of-custody, and risk management. Evaluated US & International acts & regulations related to FISMA, GDPR, HIPAA, SOX; FIPS, ISO 27000 series, and PCI-DSS 3.1 standards; industry best practice; COBIT 5, and NIST-SP-800 guidelines. Director America Tech, Inc - Silver Spring, MD October 2013 to August 2015 IT, Cybersecurity, Privacy, Audit, Risk Management & Regulatory Compliance) Responsibilities: Directed and managed the information technology (IT), information security, database management, cybersecurity, cloud security, data privacy & data protection, identity theft prevention, and HR activities. Designed the secure architecture, sales, SOC, NOC, agile & secure software development life cycle (SSDLC), PIA, network & wireless security, e-Commerce, e-Governance; FTK, EnCase & TableAU imaging; ProDiscover, digital forensics, e-Discovery, chain-of-custody, penetration testing & ethical hacking, CSAM, internal & external audit, risk management, and regulatory compliance processes. Implemented the secure communication, multi factor authentication, public key infrastructure (PKI), and identity & access management (IAM). Administered the firewalls, DMZ, intrusion detection & prevention systems, and virtual private network (VPN). Monitored personally identifiable information, protected health information & data breaches. Developed organizational strategic standards, policies, procedures, and guidelines. consultant (Global Program Manager & Risk Controller) Served Deutsche Bank February 2015 to March 2015 in IT risk management, security audit analysis, and regulatory compliance. Intensively worked on the evaluation & implementation of key risk indicators (KRI), effect of existing security & financial laws and regulations, security strategies, security policies & procedures, and industry best

practices. Analyzed Securities Exchange Act of 1934, Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), Federal Information System Controls Audit Manual (FISCAM), and Assessing Security & Privacy Controls in Federal Information Systems & Organizations: Building Effective Assessment Plans (NIST-SP-800-53A). Designed, developed, and documented a risk management & mitigation framework with recommendations on information assurance, cybersecurity, privacy, and continuity of business operations (COOP). Developed security categorization (SC) plan, configuration management plan (CMP), information system security plan (ISSP), continuity of operation (COOP) plan, contingency plan (CP), and incident response (IR) plan. Conducted FISMA audit, CP tests & drills, vulnerability scanning, privacy impact assessment, awareness, training, IV&V, gap analysis, security testing & evaluation (ST&E), plan of action & milestones (POA&M), ATO, business impact assessment (BIA), certification & accreditation (C&A), and assessment & authorization (A&A). Used CSAM tool. Coordinated change control management, change control board (CCB), patch management, and customer relationship management (CRM). Used Cain & Abel, AVG, Nessus, MBSA, Zenmap, Nmap, Kleopatra, and Wire Shark tools. Planned, designed, tested, installed, and implemented a sophisticated & comprehensive Cybersecurity Laboratory for conducting vulnerability scanning, penetration testing (ethical hacking), intrusion detection & prevention, disaster recovery (DR), incident response (IR), backup & recovery, imaging, business impact assessment (BIA), digital forensics, e-Discovery, and chain-of-custody for cyber defense and safeguarding critical assets. Conducted digital asset management. Worked on cryptocurrency, blockchain, and IoT security. Counselled five corporations in Washington DC area on analyzing RFI & RFP from Department of Homeland Security, Department of Interior, Department of Commerce, Federal Deposit Insurance Corporation, etc. in business development. Developed and implemented project plans. Director IDGMI - Miami, FL June 2013 to October 2013 IT, Cybersecurity, Privacy, Risk Management, Sales, and Regulatory Compliance) Responsibilities: Directed and managed the designing, developing, and customer relationship of national & international consultancy services in information technology, information security, cybersecurity, SOC, data privacy & data protection, identity theft prevention, network &

cloud security, healthcare information security, identity control & access management, PKI, multi factor authentication, e-Commerce, backup & recovery, contingency planning (CP), incident response (IR), continuity of operation, disaster recovery, business impact assessment, Sarbanes-Oxley Act (SOX), external & internal audit, risk management, and regulatory compliance. Conducted IV&V, gap analysis, security compliance testing, and privacy impact assessment (PIA) for the Health Exchange Program of Hawaii State Government and its stake holders (State Healthcare Providers & Insurance Companies) using the Center for Medicare & Medicaid Services guidelines. Designed and supervised the secure software development life cycle (SSDLC) of the IDGMI info systems. Program Manager (Security Assessment & Authorization, Information Security & Privacy) B3 Solutions, LLC - Alexandria, VA November 2010 to June 2013 901 N. Pitt St., Suite 300, Alexandria, VA 22314, USA Duration: 11/2010 to 06/2013 Role: Program Manager (Security Assessment & Authorization, Information Security & Privacy) Responsibilities: Was responsible for secure software development life cycle (SSDLC) & agile; policy, procedures, infrastructure, architecture, SOC, NOC, forensics, cryptocurrency, blockchain, IoT, cybersecurity, cloud security, data privacy & data protection, identity theft prevention, PIA, e-Commerce, identity control & access management, PKI, MFA, SOX, external & internal security audits, IV&V, gap analysis, validation, continuous monitoring, POA&M, ATO, C&A, assessment & authorization (A&A), hardening, patching, IT risk management, and regulatory compliance. Completed A&A of seven (7) DHS systems (FLETC Collaboration System, Information Security Architecture, Financial Accounting & Budgeting System, Internet System, Emergency Security Solution, Artesia Administrative Network, and Environmental Data Integration System) and four (4) FAA systems (System Architect, Logical Access & Authorization Control Service, Information Security Business Portal, and Investment Management Tools). Worked on business development. Implemented regulations, OMB circulars & memorandums, FIPS & ISO 27000 series standards; FISMA, SOX, FLETC, FAA, DOT, DHS orders; NIST guidelines; CSAM & TFA tools; industry best practices. Designed, developed, reviewed, examined & tested security policies, procedures, configuration management, incident response (IR) & contingency plan (CP) and their training & testing; IT risk assessment, system

security plan, change management process, security posture, disaster recovery, continuity of operation, business impact analysis, security categorization, privacy threshold analysis, privacy impact assessment, security testing & evaluation, plan of action & milestones, security assessment, authorization (ATO) or denial memorandum. Worked in customer satisfaction & retention. Designed "Cybersecurity, Privacy & Information Assurance" laboratory for B3 Solutions. Attended management retreat, 5/15 years corporate strategic planning, and contributed in the business development drills. Developed technical contents to respond RFP. Program Manager (Information Security, Privacy, and Risk Management) Digicon Corporation - Herndon, VA October 2009 to October 2010 510 Spring Street, Suite 100, Herndon, VA 20170, USA Duration: 10/2009 to 10/2010 Role: Program Manager (Information Security, Privacy, and Risk Management) Responsibilities: Subject matter expert (SME) in cybersecurity, information assurance, IT risk management & risk management frameworks; regulatory compliance (FISMA, HIPAA, GLBA, SOX, OMB, FISCAM, FIPS, ISO 27000 series, etc.); certification & accreditation (C&A), IT governance, NIST-SP-800 guidelines (800-30, 800-34, 800-37, 800-39, 800-47, 800-53, 800-53A, 800-60, 800-83, 800-87, 800-100, 800-122, 800-137 and 800-153), security policies & procedures, enterprise security architecture, cloud security, security programs, IAM, personally identifiable information, privacy impact assessment, awareness, training, disaster recovery, COOP, incident response (IR) & contingency plans (CP), their tests & drills and business impact assessment (BIA). Was responsible for cross functional teams, technical guidance, agile & secure software development life cycle (SSDLC), SOC, NOC, program management, risk assessment, staff training & mentoring, cybersecurity, PII, PHI, PIA, data privacy & data protection, identity theft prevention, and customer satisfaction. Conducted FISMA audit, security testing & evaluation, continuous security monitoring, hardening, patching, IV&V, and gap analysis. Developed computer-based training (CBT) on incident response, configuration management, security categorization, systems security plan, security assessment report, plan of action & milestones, ATO, and executive summary. Facilitated, communicated, and reported program activities. Completed C&A of five information systems of ARP & AST line-of-business of FAA. Was author of CSAM (Cyber Security Assessment & Management)

tools for risk assessment & POA&M management. Worked in RFP analysis, technical writing, sales, and IT business development. Program Manager Earth Resources Technology, Inc - Laurel, MD March 2009 to October 2009 Risk Management & Regulatory Compliance - NOAA/NESDES project) Responsibilities: Served as a SME in agile & secure software development life cycle (SSDLC), information security, security architecture, cybersecurity and both phases of C&A (certification & accreditation). Was responsible for recruiting, technical guidance, NIST implementation, tasking, awareness, training, facilitating, mentoring, delivering, reporting, customer satisfaction. Provided ISO 27000, FISMA, FISCAM, OMB, regulatory compliance services, and program management. Guided & conducted security categorization, vulnerability scanning & reporting, system security plan (SSP) development, FISMA regulatory compliance, external & internal security audits, contingency plan (CP), incident response (IR) plan, disaster recovery plan, continuity of operation plan, exercises, and risk assessment; PII, PHI, PIA, data privacy & data protection, and identity theft prevention; IV&V, gap analysis, security testing & evaluation, hardening, patching, plan of action & milestones (POA&M), certification & accreditation (C&A), A&A, ATO, and continuous monitoring for critical infrastructures, major applications, general support systems, and industrial control systems. Reviewed policy & procedures and implemented risk management framework. Director EKTI Group of Companies, Inc - Laurel, MD July 2007 to March 2009 IT, Cybersecurity, Privacy, Risk Management, and Regulatory Compliance) Responsibilities: Served the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) & the Department of Commerce (DOC) as a Lead C&A Consultant & Subject Matter Expert (SME) in secure software development life cycle (SSDLC), information assurance, cybersecurity, data privacy & data protection, security architecture, FISMA audit & CSAM tools. Contributed in policy, procedures, security categorization, system security plan, access & audit controls, IAM, PII, privacy impact assessment (PIA), contingency plan (CP), incident response (IR) plan, disaster recovery plan (DRP), COOP, tests & exercises, security testing & evaluation, plan of action & milestones, security assessment report, ATO, certification & accreditation (C&A), awareness, training, IV&V, gap analysis, risk based decision, continuous monitoring, and customer relations. Conducted risk assessment, vulnerability & threat analysis,

configuration management, business impact assessment, and security posture determination. Counseled system owners, information system security officers & contingency coordinators on security governance, intrusion detection & prevention, e-authentication, secure communication, encryption, vulnerability scanning, patch management, incident reporting, digital forensics, chain-of-custody, media sanitization, and digital signature. Implemented FISMA, FISCAM, OMB, SOX, GLBA & other regulatory compliance; NIST guidelines, FIPS standard & industry best practices. Developed & validated MOU, service level agreement, standard operating procedures & interconnection security agreements. Analyzed concept of operations, security architectural designs and requirement traceability matrix. Assured least privilege, separation of duty, hardening & defense-in-depth. Contributed to change control board, architectural working group, secure software development group & business development. Chief Information Security Officer (Cybersecurity, Risk Management, and Compliance) HeiTech Services, Inc - Landover, MD November 2006 to June 2007 8201 Corporate Drive, Suite 600, Landover, MD 20785, USA Duration: 11/2006 to 6/2007 Role: Chief Information Security Officer (Cybersecurity, Risk Management, and Compliance) Responsibilities: Established strategic vision and business planning in IT, information security, cybersecurity, data privacy & data protection, identity theft prevention, PIA & risk management. Supervised SOC, NOC, IAM, NIST implementation. Participated in secure software development life cycle (SSDLC) & risk management. Implemented SOX, GAO, FISMA, OMB, FISCAM, HIPAA, PCI DSS and other regulatory compliances. Served as the subject matter expert (SME). Developed policies, procedures and step-by-step guidelines. Completed FISMA audit, IV&V, gap analysis, ST&E, POA&M, ATO and C&A of FLETC (Federal Law Enforcement Training Center) information systems of the Department of Homeland Security (DHS). Updated system security plan. Developed contingency plan (CP), incident response (IR) plan, emergency plan, DRP and COOP. Conducted tests & exercises. Contributed in sales, CRM, and business development. subject matter expert (SME) Dakota Consulting Inc - Silver Spring, MD March 2006 to November 2006 9700 Lorain Avenue, Silver Spring, MD 20901, USA Duration: 03/2006 to 11/2006 Position: SME (Information Security, C&A, IT Risk Management, and Regulatory Compliance) Responsibilities: Served as a

subject matter expert (SME) in cyber security, risk management, secure application development, data privacy, PKI, and multi factor authentication at OPM & USDA; implemented FISMA, FISCAM, OMB, FIPS, NIST-SP-800, and other regulatory compliance, standards, and guidelines; developed security policy, procedures, system security plan (SSP), contingency plan (CP), and disaster recovery plan; conducted CP excises; monitored security control, access control, personally identifiable information, privacy impact assessment, IV&V, gap analysis, business impact analysis, change management, ST&E testing, POA&M management, and certification & accreditation (C&A) of Learning Management Systems (LMS). Principal Analyst (IT Security, Privacy, Risk Management & Regulatory Compliance) Project Performance Corporation - McLean, VA July 2005 to January 2006 PPC), 1760 Old Meadow Road, McLean, VA 22102, USA Duration: 07/2005 to 01/2006 Position: Principal Analyst (IT Security, Privacy, Risk Management & Regulatory Compliance) Responsibilities: Worked for the DOI; assigned tasks to the team & ensured quality of delivery; kept security documents updated; performed risk assessment & gap analysis; managed plan of action & milestones, coordinated training; developed contingency plan, incident response plan, and C&A guidelines. Contributed to secure application development, FISMA, SOX, HIPAA, and privacy compliance; security plan, risk management, security control matrix, secure architecture. OnPoint Corporation - Arlington, VA November 2004 to July 2005 Position: Information Security PM (C&A for NIH & Maryland State Voting; IV&V for USDA) Responsibilities: Implemented FISMA, FISCAM, OMB & other information security regulatory compliances; conducted risk assessment, independent verification and validation & gap analysis of 200+ information systems of USDA - evaluated system security plans (SSP), security self-assessments, incident response plans, security testing and evaluation results, plan of action and milestones, trusted facility manuals, security features user guides, contingency plans, systems control compliance matrixes & privacy impact assessment. Conducted IV&V and gap analysis on the risk assessment documents of the State of Maryland Voting Systems. Conducted C&A of a NIH system. Evaluated & validated SSP, ST&E, POA&M & other C&A deliverables to NIH. Information Security Analyst (C&A, Policy and Procedures, and FISMA Compliance) Avineon Inc - Alexandria, VA August 2004 to October 2004 4825 Mark Center

Drive, Suite 700, Alexandria, VA 22311, USA Duration: 08/2004 to 10/2004 Role: Information Security Analyst (C&A, Policy and Procedures, and FISMA Compliance) Responsibilities: Served U.S. Mint. Worked on ST&E, risk assessment, SSP, policy, SOP, PTA, PII, PIA, CP, IR, MOU, ISA, awareness, training, exercises (full details are available on demand). Project Manager (Business Software Development, Integration, and Implementation) Cambridge Associates, LLC - Arlington, VA March 2000 to April 2002 4100 N. Fairfax Drive, Suite 1300, Arlington, VA 22203, USA Duration: 03/2000 to 04/2002 Role: Project Manager (Business Software Development, Integration, and Implementation) Responsibilities: Developed a secure financial system; managed risk assessment, awareness, training, contingency planning, and regulatory compliance (full details are available on demand). Systems Analyst, Database Engineer, Network Administrator, and Analyst Programmer Environmental Health and Safety - Baltimore, MD May 1991 to January 2000 714 W. Lombard St., Baltimore, MD 21201, USA Duration: 05/1991 to 01/2000 Role: Systems Analyst, Database Engineer, Network Administrator, and Analyst Programmer Responsibilities: Managed network; initiated, analyzed, designed, programmed, tested, validated, integrated, deployed, managed, maintained 3 applications (full details are available on demand). Database Developer Johns Hopkins University and Hospital - Baltimore, MD June 1990 to April 1991 615 N. Wolfe St., Baltimore, MD 21205, USA Duration: 06/1990 to 04/1991 (Full-Time) and 06/1995 to 05/1996 (Part-Time) Position: Database Developer, Vaccine Testing Unit of the Department of International Health Responsibilities: Developed 3 interactive database application systems for vaccine trial, vaccine testing, and health care projects of Johns Hopkins Hospital, Johns Hopkins Travelers Clinic, and Navajo Vaccine Trial Projects; performed users' requirements analysis, system design, coding, acceptance testing, integration, deployment, users' training, and maintenance; developed user's guide, IT contingency plan; managed vaccine trial databases, and generated management reports. Education Graduate Certificate in Cybersecurity in GCC University of Maryland 2012 MS in Information Systems in Management University of Maryland 1999 BS in Information Systems Management University of Maryland 1997 Skills Active directory, Encryption, Fisma, Hipaa, Incident response, Pci, Gap analysis, Life cycle, Software development life cycle, Cobit, Data protection,

Disaster recovery, Glba, Information security, Iso, Iso 27000, Nist, Pki, Sox, Software development Additional Information RELATED SKILLS - SME (Subject Matter Expert) in information technology (IT), information security, information assurance (IA), database management, DBA, IT risk management, active directory; cybersecurity policy, procedures & strategic planning; security audit & assessment, and continuous monitoring - SME in encryption, data privacy, data protection, digital forensics, asset protection, e-Discovery, chain-of-custody, presentation, pre-sales & post-sales consultancy, e-Commerce & e-Governance - SME in system security plan, security categorization, security testing & evaluation, plan of action & milestone; awareness, training, and education; IAM, C&A, assessment & authorization (A&A) - SME in vulnerability, cyberthreat, cybercrime, cybersecurity and critical infrastructure protection - SME in agile, secure software development life cycle (SSDLC), intrusion detection, IV&V, gap analysis, configuration management, defense-in-depth, defense-in-breadth, business development - SME in enterprise security architecture, network scanning, emergency preparedness, incident response (IR) and IR drills, COOP, disaster recovery (DR), and business impact assessment (BIA) - SME in security acts, circulars, memorandums, and regulatory compliance (ISO 27000 series, OMB, FISMA, FedRAMP, SOX, HIPAA, GLBA, COBIT, FIPS standard, PKI, AWS, and Azure) - SME in NIST Special Publications (SP) including 800-30, 800-34, 800-37, 800-39, 800-53, 800-53A, 800-61, 800-83, 800-94, 800-114, 800-122, 800-137, 800-144, 800-161, 800-183, 800-184 - SME in GDPR, IoT, PCI DSS, PII, PHI, identity theft prevention, privacy impact assessment (PIA), healthcare security, contingency plan (CP), CP drills, ISO 26262, and automotive security -15 years of experience in teaching Cybersecurity, Privacy, and Technology classes at Universities

Name: Jerry Avery

Email: ggolden@example.com

Phone: 241.558.6560x982