IT Risk Manager IT Risk Manager Information Security Expert Riverview, FL 25+ years in information technology consulting and leadership experience. Primary skillset: + Assessing and Auditing IT Security Controls. Including: Administrative (policies, standards and procedures) Technical (Infrastructure Devices, Servers, Databases, Workstations, Portable Devices and other IT components) Physical (Data Centers, UPS Systems, Fire Protection Systems, Access Controls) Practices and Technology related to preventive, detective and corrective controls to reduce risks to Confidentiality, Integrity and Availability of IT and business assets + Planning and Implementing IT Security Controls. Including: Policies, Standards and Procedures Intrusion Prevention Systems Security Event Management Systems Firewalls, VPNS, Routers and Switches User Awareness Training Disaster Recovery & Business Continuity + Sales and Marketing of IT Security: Write Statements/Scope of Work Consult with clients and build business cases for investments in IT security controls Specialties: + Expert Knowledge of Regulations, Security Standards and IT Frameworks: CISSP CBK ISO 27001/27002 COBIT ITIL GLBA NCUA HIPAA HITECH PCI SOX OWASP NIST Special Publications GDPR --- Authorized to work in the US for any employer Work Experience IT Risk Manager Holland & Knight - Tampa, FL June 2018 to Present Key Responsibilities Include: Assist in the maturation and management of the Threat and Vulnerability Management program. Scan systems for known vulnerabilities and provide support in the remediation of any vulnerabilities found. Identifies areas of security risk, determines risk level and assists with efforts to mitigate those risks to an acceptable level. Measure and report on security posture through the ongoing development and refinement of security metrics. Performs issue and problem resolution and general security operations support. Assists with security-related investigations and incident response activities and provides system forensics and investigative services. Provide periodic on-call support of security operations during non-business hours. Review change requests from a security perspective, understand and determine associated risk levels and make recommendations for approval or denial based on the risk presented. Ability to understand, prioritize and complete tasks by working independently or with a team. Review, recommend and assist in implementing proper security diagnostic and access tools to enable the analysis, reporting and escalation of security events.   Act as a point of contact for execution for vulnerability testing of networks, systems and applications as requested.   Assist in the growth and development of the incident response team to act quickly and accurately during emergency situations.   Participate in the development, and delivery of an information security awareness program.   Approaches all problems, projects, and incidents with a high level of professionalism, objectivity and an open mind to new ideas and solutions.   Analyzes and identifies areas where automation can be used in the deployment of new technology to support effective resource management.   Maintain knowledge of vendor products, services and security technologies and recommend/implement their use.   Lead the implementation of ISO 27001 through certification. IT Security Architect/Manager Global Convergence Inc - Oldsmar, FL April 2017 to June 2018 The Security Manager oversees all facets of the company s security and data privacy program and controls. Recommends, designs, and maintains security and risk controls in alignment with the company objectives, strategies, and/or contracts, implements policies and training procedures. Responsible for all information technology and physical security management including policies and procedures, employee security awareness and training, metrics, technical design and controls, and implementation. Provide security consulting services, as needed, to various projects and serve as a subject matter expert with regard to information and physical security architecture.   Oversees, facilitates, validates, and prepares security and audit materials or reports as required. Stays abreast on the latest industry trends and best practices in IT information security to protect the organization s computer networks and systems.   Responsibilities: Multi-layer information systems with understanding of modern applications, databases, internet/web and system architecture   Common operating systems and business application platforms with an understanding of enterprise architecture and integrations   Network security, configuration, protocols, and standards   Future trends within areas of expertise and understanding of converged security and risk management technology   Physical facility and data center security   Strong technical and cross functional relationship building skills with the ability to interact with inside and outside subject matter experts

Encryption schemas and algorithms, various authorization and authentication mechanisms/software, network monitoring and sniffing, and vulnerability and threat management tools Security controls design, implementation, validation, and auditing procedures Regulatory requirements, industry compliance, and security standards such as PCI DSS, ISO 27001 and ISO 9001, SOC1, SOC2, and GDPR Implemented security tools to address gaps and requirements (Rapid 7 InsightVM, Rapid7 InsightIDR, CarbonBlack Protect/Bit9, Forcepoint/Websense, Okta, Thycotic Secret Server, Microsoft SCCM, MalwareBytes, Symantec Endpoint Security, CISCO TACACS+, ZenGRC etc.) Information Security Risk Consultant Tenet Healthcare - Remote September 2015 to May 2017 Responsibilities Served as an internal information security consultant to each facility (e.g. hospital, ambulatory practice, outpatient center, etc.) Initiated, facilitated, and promoted activities to create information security awareness within the facilities Focused extensively on building and expanding relationships with key stakeholders such as market/facility leadership, physicians, other markets security analysts, business partners and vendors Supported information security assessments, acting as a liaison to Internal Audit, Compliance, and the corporate security teams Supported information security assessments of vendors security controls Supported information security assessments for potential mergers and acquisitions, working with Business Development as needed Supported external auditors as needed, including system-wide access, policy review and remediation Monitored compliance with information security policies and procedures, referring problems to the appropriate department manager Provided direct training and oversight as needed, ensured proper information security clearance in accordance with established organizational information security policies and procedures Identified/assessed business process and IT risks, design appropriate audit steps and plan, execute and wrap up audits Sr. Information Security Analyst WellCare - Tampa, FL May 2016 to December 2016 Defined and established a governance structure to include a steering committee and associated workgroups (as necessary), to support collaboration, communications, decision making, prioritization, accountability related to IAM investments and services at WellCare. Determined the appropriate structure, charter, and work plan for the Steering Committee. Established the governance structure within WellCare and determined the appropriate stakeholders, setup and conducted interviews, gathered buy-in and support for an IAM steering committee. Drafted a steering committee charter to document the purpose, structure, and cadences of the committee. Worked with vulnerability management team to establish vulnerability management program, track remediations and document risk. Developed baseline security standards and minimum secure configurations. Information Security and Risk Management Consultant PwC - Tampa, FL November 2015 to April 2016 Responsibilities Leveraged knowledge of risk identification, assessment, treatment processes to contribute to the development of new domain expertise in those processes on an ongoing basis. Developed access control policies and a strong knowledge of role based access through the use of enterprise class user entitlement systems. Conducted internal assessment audits, including communication of findings, development of corrective action plans, and tracking corrective action status. Incorporated assessment and audit findings into ISMS risk assessment processes. Managed policy management, risk management, and document management applications to develop and maintain security policies and standards. Identified and leveraged relationships between data held in different applications to develop tools and reports that support the management of information security. Contributed to cross-functional efforts, working with business, IT and global teams, as a representative of the risk management organization. Responsible for leading cross functional teams. Responsible for managing work by suppliers and other providers. Worked closely with US and global risk management, security and IT organizations Information Security Architect Hillsborough County Aviation Authority (Tampa Airport) - Tampa, FL June 2015 to November 2015 Responsibilities Performed highly complex analysis and technical tasks involving assignment and coordination of measures to provide information assurance, event detection and rapid response across various environments of the enterprise. Designed, implemented and supported integration of information security solutions including security architectures, firewall administration/monitoring, integrating security products, and developed and coordinated security implementation plans. Guides users and technical team members in formulating security requirements, integrating security requirements into existing system architectures, developing security test plans, overseeing the execution of security testing, and advising on alternative approaches. Provided technical lead on security projects which involved a wide range of issues including secure architectures, secure electronic data traffic, network security, platform and data security and privacy. Provided organizational support of enterprise security architecture and design, benchmarking, technical framework and gap analysis. Reviewed and contributed to the improvement and standardization of the security administration process across all business units. Prepared training plans for staff, allocated ongoing training for personnel on new computer systems or technologies being implemented which required security administration. Assisted in forensic analysis, security incident response and investigations. Performed daily Security Alert and Log Monitoring (Central Log, Virus, IPS, DLP, Web Content, Secure Email, and Active Directory Changes). Assisted with Monthly alert and log management reporting. Information Security Analyst -Remote HP - Austin, TX February 2015 to June 2015 Responsibilities Assisted in the demonstration of system security operational objectives by contributing information and providing recommendations to strategic plans and reviews. Assessed systems for compliance against aligned security policies and standards and conducted gap analyses. Prepared and completed associated remediation action plans; assisted with resolving problems; identified trends; determined system improvements and drove needed change. Recorded system security plan information in the eGovernance, Risk and Compliance application to promote and develop security strategies; directed system control development and access management, monitoring, control, and evaluation. Assessment and understanding of system safeguards, security provisioning and disaster preparedness and test plans. Advised senior management by identifying critical security issues; recommending risk-reduction solutions. Information Security Analyst/Consultant Liberty Medical Supply - Port Saint Lucie, FL July 2014 to February 2015 Responsibilities Complete implementation of existing security tools and controls (SIEM, Endpoint security, firewalls, web filtering, email filtering, etc.) Rewrite security policies and procedures. Conduct security gap analysis and risk assessment. Recommend and implement new security technologies (DLP, IPS, Endpoint, SIEM, Malware, content filtering, etc.) Review and advise on new software, hardware and vendors. Develop and implement incident response plan and process. Information Security Analyst/Consultant Chico'sFAS - Fort Myers, FL March 2014 to June 2014 Responsibilities: Perform information security reviews of requirements statements, detailed designs, implementation plans, and other documents produced during the systems development process. Evaluate and recommend improvements to controls associated with information technology-related business processes such as: acquisition of information systems hardware and software, proper segregation of duties, application system development and testing, as well as systems change management. Conduct qualitative and quantitative business systems risk assessments; findings presented to senior management. Lead security projects including requirements definition, task planning, research, testing, implementation, and management. Prepare and periodically update information security policies, architectures, standards, and/or other technical requirement documents needed to advance application security. Perform periodic information systems risk assessments including those associated with the development of new or significantly enhanced business applications. Assist in developing security awareness materials, security presentations, and information security training sessions. Sr. Information Security Analyst/Consultant Everbank - Jacksonville, FL June 2013 to January 2014 Responsibilities: Developed information security standards, policies, procedures and best practices. Planned and implemented access control measures including privilege management, access provisioning/de-provisioning, and periodic entitlement reviews. Performed risk assessments. Planned and implemented application and system security standards, and configuration compliance. Planned and implemented security awareness including multi-media messaging campaigns, and formal compliance training. Researched the latest information security trends and emerging threats. Participated in vendor security assessments. Supported the information security program mission by completing related tasks as needed. Sr. Information Security Analyst/Consultant Citizens Property Insurance - Tallahassee, FL November 2012 to June 2013 Responsibilities: Integration and requirement analysis for Application Security. Created risk assessments and risk validation in the Application Environment. Attended to all application meetings where Application Security is pertinent. Reviewed pre-existing Application Projects, and technological documents associated with the projects. Communicated and reported issues, status, and results to IT Security Management and Project teams. Foster relationships with development and technology teams to determine if additional requirements are needed during deployment of application projects. Participated in all change request meetings in respect to the application projects Remained informed on any new updates with the project. Became familiar with the relevance of standards and policies of organization Developed and managed Risk Management processes and documentation Enhanced risk assessment process, updated documentation and deliverables, and migrated to GRC platform Matured Risk Management program to better align with standards. Standards in use: COBIT as governance framework, ISO 2700x for operational controls, NIST for process and documentation standard, ITIL for service delivery Information Security Officer Sabadell United Bank - Miami, FL November 2010 to November 2012 Responsibilities: Developed and implemented Information Technology and Information Security Policies, Procedures, and Standards. Lead and executed audit assignments in accordance with established project plans and audit programs, ensuring consistent quality in communication, execution, and delivery of objectives. Developed security processes and procedures and supporting service-level-agreements to ensure that security controls are managed and maintained. Developed and implemented reports to ensure that security controls are managed and maintained. Worked with the IT department to identify, select and implement technical controls. Worked with all business units and with other risk functions to identify security requirements, using methods that included risk and business impact assessments. Worked with business units and vendors to identify security control requirements, establish assessment process and address/remediate weaknesses. Performed application (.NET environment) and infrastructure security assessments. Coordinated with application development and network/systems teams to establish remediation plans, and validate remediation actions. Researched and assessed new threats and security alerts and recommended remedial action. Developed strategies and plans to achieve security requirements and address identified risks. Kept management informed of audit project status and challenges as they arise. Assisted the CTO in budgeting for security analysis and security related implementation tasks. Published implementation guidelines and templates. Coordinated with department managers to perform reviews of key business processes with underlying information systems. Assisted with Vendor Management planning, testing and documentation. Assisted with Business Continuity planning, testing and documentation. Assisted with Change Management policies, procedures and documentation. Reorganized and developed policy framework to align with ISO 27002:2005. Developed risk assessment strategy derived from NIST 800-30. Aligned IT Security practices to corporate framework built on COBIT 4.1 Addressed compliance requirements of FDIC, OCC, and external auditors. Drafted policies to address gaps within the organization and address weak policy statement areas. Managed Web Content Filtering Proxy (WebSense). Managed Active Directory Security and Group Policy. Supported Endpoint Protection and DLP project teams (Symantec and McAfee). Supported Vulnerability and Patch Management remediation (Rapid7, Nessus, WSUS, PatchLink). Managed information security around perimeter defense and various security appliances. Supported multiple technology teams from an information security perspective. Senior Security Consultant Insight Direct - Client: HAMILTON COUNTY SCHOOL DISTRICT - Tampa, FL June 2010 to November 2010 Network Security Implementation Access Control Lists (ACLs). Identified School and Administrative User Functional Groups. Identified Network Asset Functional Groups. Designed ACLs to match Functional User Groups to Network Asset Functional Groups mappings. Implemented ACLs in remote and Administrative facilities, Data Center and CoLo Tested ACL configurations. SNMP Reconfiguration Identified all devices that require SNMP access. Identified all devices that only support SNMP v1, remediate as necessary, case by case. Identified all devices that will access the SNMP information and users associated with these devices. Designed SNMP Configurations for the network devices to map access with the management and administrative workstations. Implemented SNMP Configurations. New Read-Only and Read-Write Community String for Network Devices. New Read-Only and Read-Write Community String for Servers. Restrictions for access to SNMP responses, authorized devices. Test SNMP reconfiguration. Wireless Network Reconfiguration and Remediation Assess needs of the Administrative Wireless Networks. Identified Wireless devices on network. Designed ACL and VLAN configurations. Designed WPA and Authentication Policy. Implemented VLANs and ACLs for authorized wireless access points. Implemented WPA and Authentication policy for authorized wireless access points. Tested Wireless Networks. Wired Port Management Consulted and documented methods of wired access restrictions (HCDE to enforce at facilities). Disabled Switching Ports. Removal of Physical Patch Cables. Senior Security Consultant Insight Direct - Client: ADVENTIST HEALTH SYSTEMS - Tampa, FL January 2010 to June 2010 Performed enterprise wide risk assessment for all SQL database instances in the environment. Developed a comprehensive inventory of the all Microsoft SQL platforms within the environment. Identified and documented owner for each instance. Identified and documented the support personnel for the instance. Which applications the SQL platform supports if applicable. Environment Identify and document the status of each instance as production vs. testing. Used a combination of open source and commercially available tools to identify the vulnerability and security risks within each of the identified SQL Server platforms. Developed remediation recommendations for the identified vulnerabilities including identifying critical SQL Server or Microsoft Windows security updates and provided direction about how to resolve them. Approximately 1200 Database Instances. Databases located in 2 Datacenters and across 35 hospitals. Information Security Architect TARGET CORPORATION - Minneapolis, MN March 2008 to January 2010 Managed vendor risk assessment projects from project initiation through remediation. Coordinated with stakeholders and relationship managers to identify, document and remediate risks at 3rd party locations in accordance with Target Information Security standards. Developed repeatable and defensible process for identifying risks, determining recommendations and assigning risk levels. Collaborated with business leaders to refine documentation and reporting to better address repeatability and consistency. Worked with various business units to establish a vendor manager training process for security and compliance. Addressed compliance issues related to GLBA/FFIEC, PCI, HIPAA, NIST 800-30 and internal controls requirements. Utilized the BITS SIG and AUP to document vendor IT Controls and document risks. Information Security Consultant Assurity River Group - Minneapolis, MN May 2006 to February 2008 Responsibilities Conduct Risk and Vulnerability Assessments Conduct Policy and Procedure Assessments Based on Regulation (HIPAA, GLBA, SOX, PCI) and Best Practices Frameworks (Cobit, ISO-17799) Author policies, procedures, standards and short-long term Risk Management strategies Conduct Information Security User Awareness Training Conduct Business Impact Analysis Create Disaster Recovery and Business Continuance Strategies Information Security Analyst WELLS FARGO February 2005 to April 2006 Reviewed and analyzed the impacts of modifications and/or additions to the Wells Fargo network. Classified data as it is defined by Wells Fargo risk level policy. Performed impact analysis and risk assessment on security plans as submitted by Wells Fargo business units. Managed projects in queue and as they progress through the information systems process from request through delivery of services. Supervised technology subject matter experts (SMEs) through each stage of the process to insure risk is mitigated and policy is followed. Developed new security plans as needed to complete documentation on each risk assumed by the Wells Fargo Home Mortgage business unit. Ensure compliance with GLBA, SOX, and ISO 17779 as necessary within each project. Consistently monitor all changes to the Wells systems, software, and network to insure that policy was followed and changes were made according to regulatory and corporate standards. Processes included site reviews of new business partners, code reviews of new or modified software systems, and topology and architecture assessments of new network connectivity as well as current architecture. Information Security Consultant ECOLAB INC - Saint Paul, MN November 2003 to January 2005 Performed security auditing and risk assessments company-wide. Established security policies and deployed intrusion detection systems on various systems throughout the network. Developed a roadmap for further advancement of security procedures. Primarily targeted known vulnerabilities and software issues (ArcServe and PCAnywhere) where needed. Reviewed Windows 2000 and 2003 Active Directory design and user security and made recommendations of change and policy updates. This was a very large virtual server environment utilizing VMware and a blend of Windows 2003 and Linux servers. Approximately 300 servers with approximately 35,000 end users. Developed specification for disaster recovery plan and recommended vendor solutions.

Utilized many open source tools (nmap, Nessus, Nagios, Snort, Tripwire, among others) to perform monitoring and analysis of network structure and security. Chief Technology Officer Maximum Bank - Minneapolis, MN September 2001 to November 2003 Education Computer Science Mankato State University - Mankato, MN 1994 to 1999 Skills Cissp, Cyber Security, Nist, Siem, Information Security, It Security, Information Assurance, Cybersecurity, Network Security, PCI, Cisa, Governance, Risk Management, Compliance Links http://www.linkedin.com/in/jasonrroth/ Certifications/Licenses CISSP CISA

Name: Dr. Matthew Gomez

Email: emmahunter@example.net

Phone: +1-390-653-9566x3478