Head of Identity & Access Management Head of Identity & Access Management Head of Identity & Access Management - Jefferson University Hospital Hockessin, DE Work Experience Head of Identity & Access Management Jefferson University Hospital - Philadelphia, PA September 2018 to Present Approachable leader who has built significant relationships with other team leaders and members; implemented and sustained improved processes in conjunction with those leaders that improved our service delivery by 80% in 90 days. Lead, manage and coordinate identity & Access Management across the enterprise, including Access Management analysts, leads, engineers, and architects Define, implement and support the Identify & Access Management (I&AM) strategy and multi-year roadmap Work across functional areas and partner with key stakeholders to ensure successful implementation of all I&AM service capabilities Lead efforts to identify business requirements for specific system, application or process changes, work with the business to ensure sound delivery of access control solutions Coach and develop team, leveraging individual strengths and positioning employees for continued growth and success Develop and maintain policies, standards and procedures revolving around permissions, security groups and methods for gaining access to information. Assist with the design, implementation, maintenance, and troubleshooting of the organization's identity and access management control systems and execution of the enterprise data management policies. Stood up reporting and monitoring processes to provide accountability and sustainability of performance, quality of service, and customer service satisfaction. Assist in the evaluation of tools to support a solid Identity and Access Management foundation. Maintain interactive relationships with members of the Information Governance, Security & Risk Management, and Infrastructure teams to ensure goals are understood, and facilitating discussion to achieve an appropriate and balanced result. Participate in change management meetings and processes. Partner with other senior leaders via Steering and Governance Committees to develop enterprise-wide internal policies, procedures, guidelines and best practices with respect to access and identity management issues. Vice President - Centralized Support Systems JP Morgan Chase - Newark, DE May 2018 to September 2018 Business Operations Manager Implemented and managed an Information Owner (IO) Center of

Excellence (COE) that followed a consistent lifecycle, supported robust training, and ensured all BAU activity was appropriately reported and governed Developed a strategic short-term and long-term roadmap aligned to a common operating model Implemented a set of governance management processes Built a robust suite of reference tools such as training guides, certifications, etc. Created a communication process and a reporting plan to monitor program health while driving continuous improvement and exam ready principles Vice President - Information Risk/Controls JP Morgan Chase - Newark, DE May 2017 to May 2018 Program / Controls Manager Provided oversight and governance for multiple business and IT control programs, end-to-end Developed and led Business Access Admin testing pilot for CCB Operations to review the design and identify the effectiveness of access controls Analyzed and Redesigned business controls to maximize coverage and reduce inherent risk across the firm Performed end to end control reviews; made recommendations to streamline controls and reduce inherent risk Partnered with the controls automation team to assist with implementing continuous access control monitoring Identity & Access Mgt. Information Risk Lead JP Morgan Chase - Newark, DE October 2013 to May 2017 Defined, implemented and supported the Identify & Access Management (I&AM) strategy and multi-year roadmap Worked across functional areas and partnered with key stakeholders to ensure successful implementation of all I&AM service capabilities Led effort to identify business requirements for specific system, application or process changes, working with the business to ensure sound delivery of access control solutions Provided oversight and governance for CCB Identity & Access Management Defined, enforced, reviewed and audit Identity & Access Management corporate policy to protect the firm from access related threats. Developed, distributed, and oversaw remediation efforts for weekly Role Based Access Control (RBAC) reports for all of CCB. Saved the firm $200,000 annually by working with an application development team to fully implement automated continuous RBAC monitoring. Assisted Cybersecurity with access related incidents/investigations. Wrote SQL report queries to obtain ad-hoc information or expand scope of RBAC. Developed and executed against the service strategy/roadmap to expand RBAC: 3,6,12,18 month plans, etc. Led a Demand Management Service Level improvement initiative to

stand up a formal Intake Process for an entire organization to streamline a resource engagement model, saving the firm approximately $100,000 annually. Led initiative to ensure all IAM tasks/activities were consistently and accurately documented to ensure business resiliency. Implemented SDLC toll gate requirements for RBAC through the "secure from the start" initiative. JP Morgan Chase, Newark, DE Information Risk/ Security Technology Control Officer Liaison to LOB and internal Audit and Compliance associates, including ongoing monitoring of open issues and action plans and corresponding metrics. Provided oversight for AD teams and senior mgt. regarding IT Risk and Control initiatives. Main interface for the Line of Business with Internal Audit; working with them to ensure IRM and AD engagement in all IT or integrated reviews, and to ensure proper action plan language, ownership and client dates are reflected in final audit reports. Managed, tracked, and presented (to senior managers) several risk and control initiatives for the Originations and Information Management towers within Mortgage Banking IT, covering the following areas: ? IT Risk Central and Phoenix CSA/ASA remediation plans, including Audit plans. ? Resiliency updates for applications with compliance of disaster recovery plans and tests. ? Identity and Access Management for compliance of DCR, ID Now, RSAM, CAA and Enterprise Password Vault (EPV). ? Application risk assessment reviews and feedback to AD teams. ? SSAP - Software Security Assurance Program, entailing Application Security Certification (ASC), Normalized Vulnerability Score (NVS), Penetration Tests, Dynamic and Static Scans. Reviewed evidence submitted for the closure of control gaps (remediation plans) to ensure compliance for the firm. Oversaw all application security controls through the application lifecycle Adjunct Instructor Delaware Tech & Community College - Wilmington, DE January 2012 to January 2014 Instruct Introduction to Computers Information Risk Analyst - IT Audit Liaison/Control Lead JP Morgan Chase - Newark, DE January 2013 to October 2013 Newark, DE January 2013 -October 2013 Information Risk/ Security Information Risk Analyst - IT Audit Liaison/Control Lead Liaison to LOB and internal Audit and Compliance associates, including ongoing monitoring of open issues and action plans and corresponding metrics. Provided oversight for AD teams and senior mgt. regarding IT Risk and Control initiatives. Main interface for the Line of Business with Internal Audit;

working with them to ensure IRM and AD engagement in all IT or integrated reviews, and to ensure proper action plan language, ownership and client dates are reflected in final audit reports. Managed, tracked, and presented (to senior managers) several risk and control initiatives for the Originations and Information Management towers within Mortgage Banking IT, covering the following areas: ? IT Risk Central and Phoenix CSA/ASA remediation plans, including Audit plans. ? Resiliency updates for applications with compliance of disaster recovery plans and tests. ? Identity and Access Management for compliance of DCR, ID Now, RSAM, CAA and Enterprise Password Vault (EPV). ? Application risk assessment reviews and feedback to AD teams. ? SSAP - Software Security Assurance Program, entailing Application Security Certification (ASC), Normalized Vulnerability Score (NVS), Penetration Tests, Dynamic and Static Scans. Reviewed evidence submitted for the closure of control gaps (remediation plans) to ensure compliance for the firm. SR. Logical Access Management Analyst Aerotek - Wilmington, DE June 2012 to December 2012 Provided recertification information across the Business - ensuring ALL users of all in scope systems have the correct levels of access, and their access is authorized Undertook annual reviews of all documentation to ensure it is up-to-date and complete and obtain business owner sign-off Performed weekly exception reporting - escalation of Unmatched accounts, overdue Deletions, and any Breaches from the automated tools of information security principles and practices On-boarded new applications into LAM according to established standards Produced Metrics / Scorecards on a regular basis, as required by management Provided information to audit, internal or external, to show all LAM processes are in place and complete with no breaches in LAM controls Demonstrated effective governance to stakeholders' Solid knowledge of information security principles and practices Performed Access management tasks to critical applications including: New Hires and terminations, Assigning RSA tokens, profile access management. Educated new hires for LAM group Followed Regulatory Compliance such as: SOX, HIPAA and PCI Security Analyst Insight Global - Sungard - Philadelphia, PA October 2011 to April 2012 Solid knowledge of information security principles and practices Performed Access Management tasks as needed to include: assigning/editing RSA tokens, DNS settings, profile access management, etc.

Installed, configured, monitored and responded to IDS, NIDS and HIDS security systems and alerts Support of Content Management and Filtering Systems. Performed special projects and tasks as needed Technical experience with: Cisco routers/switches, SSH, SNMP, DNS, FTP, Syslog, SMTP, UNIX, LINUX, SQL Server, Windows 2003/2008 Server administration including Active Directory Services. Education Bachelor of Science degree in Computer & Network Security in Information Systems Security WILMINGTON UNIVERSITY Skills Disaster recovery, Firewall, Data integrity, Sql, Operations, Operations management, Training, Powerpoint, Word, Writing skills, Forensics Additional Information Dynamic and resilient professional with solid experience in fraud investigations, IT / information security, physical security, operations management, and project management. Professional skills encompass: Project management Physical security IT Security Operations management Staff supervision Education Fraud analysis/detection Staff education Public speaking Fraud investigations Mentoring Program management Other Experience and Skills 10 years of management / operations management experience 15 years' total Physical and IT security experience coupled with Law Enforcement training Excellent PC, word processing, PowerPoint, and spreadsheet skills SQL script writing skills Other Experience, Training and Coursework Human relations Basic and criminal investigation Criminal law and related matter Computer forensics Data integrity and disaster recovery Protecting your network: Firewall and perimeter security Web and data security Cyberlaw Computer Forensics training with Pro-Discover Maryland State Police Academy

Name: Anthony Wilson

Email: james21@example.org

Phone: 597-687-2552x1200