Senior IT Risk, Audit, and Compliance Analyst Senior IT Risk, Audit, and Compliance Analyst Senior IT Risk, Audit, and Compliance Analyst - BNP Paribas Pittsburgh, PA Background encompasses over 18 years of corporate information security architecture and auditing experience with Madison Bridge Management preceded by 27 years with Department of Defense as Senior Staff level compliance and auditor for the government Inspector General's office. In-depth experience in information system security design, including auditing access controls, database management, operating systems and general controls for various Payroll and Financial Services, HealthCare, and Government information systems. Technical skill sets in auditing, administration, maintenance, and implementation of various applications (App) and operating systems (OS) to include, but not limited to; Windows Server 2003-2008; Red Hat Linux; HP-UNIX and SUSE (Solaris); Identity Access Management solutions, Novell, BMC, Sun Java and Oracle IAM. Managed IS auditing (IG) team for US Air Force Reserve Command that consisted of 32 locations. Strong focus on identity access management solutions, access controls, change management processes, and risk management using DIACAP (DoD Instruction 8510.01) through the entire Software Development Life Cycle (SDLC). COBIT 5.0 Implementation CISA/CISM Certification Trainer ISACA Examination Item Writer IS Auditing Standards Champion Budgeting / Forecasting / Reporting Access Control Design/Implementation IT Security Cost Reduction Initiatives Internal Controls and Procedures Malware Management (Includes Symantec; McAfee; Trend Micro; and Sophos) FISMA Review and Implementations HIPAA and HITECH Compliance Requirements Identity & Access Management Security Architecture Design Sarbanes-Oxley Testing Designs (SOX) PCI-DSS Version 3.0 Reviews/Audits Network Security Audit Reviews ISO2700-1/2; SSAE 16; ISAE 3402 IT Security Product Implementation/TOC Firewall Design and Compliance Reviews NERC; Utilities DITSCAP Vulnerability Assessment using Open Source/Tripwire Monitoring Vendor Management Assessments Government and Private Contract Reviews Change Management/ITIL Work Experience Senior IT Risk, Audit, and Compliance Analyst BNP Paribas January 2018 to Present Provided guidance to Risk and Compliance VP for developing a Risk Management Framework RMF, which will meet the FFIEC requirements for a Level 3 maturity

organization in 2018. Performed Risk Assessment on operational teams utilizing 27001/2 and NIST 800 Frameworks Assists the Risk, Audit, and Control (RAC) team in assessing controls over operations teams within the Americas Information Security Organization. Assisted IAM teams in defining roles and responsibilities for over 300 systems building RBAC templates. Provides consultative support in the migration from current risk tracking system to RSA Archer GRC system. Assisted IAM and UOM teams in support of provisioning and de-provisioning of access to over 300 applications. Developed and wrote operation and maintenance policy and procedures for Privileged Access Management for use with SailPoint IQ to include Internet facing web applications. Working with 3rd Party Compliance leveraging Archer's series of risk assessment questionnaires to help assess BNP Paribas's third parties' control environments and collect relevant supporting documentation for further analysis. Performed analysis of the results of 3rd party questionnaires to determine BNP's organizational residual risk across several categories. Provided operation and maintenance of SailPoint IQ deployments across all BNP business units within BNP America, Canada, and Latin America (LATAM). Independent Consultant MBM CONSULTING - Pittsburgh, PA January 2003 to Present Information Technology Security Consultant and Auditor conducting project-based security assessments/audits for various global markets (Education, Transportation, Retail, Financial Services, HealthCare, and Government Agencies). Projects include building security compliance and audit programs for four data centers that were dispersed internationally and performing knowledge transfer to internal IT auditing functions to streamline the manual process. Create and implement processes for providing access control functionality through role-based (RBAC) Identity Management solutions, such as SailPoint and Oracle IAMd. Also, teach CISA training for entry-level IT auditors and CISM training for seasoned security professionals. Achieved key objectives to date, include: Designing and implementing of a global security strategy estimated at $30 million, with completion and savings of $7 million and nearly 10 months early. Initiating automated risk assessment processes, utilizing COBit and ISO27001/2 standards, saving 12-15 months from previous compliance/audit schedules. Migrating Information Security Operations and Administration team from outsourced solution to in-house solution and transferring first level security

help desk functions to offshore solution 4 months short of required project end date. Developing an IAM roadmap for the implementation of an Enforcement and Eligibility System that would support the Health Information Exchange requirements. The project was funded through Federal grant money at $136 Million dollars to support Online Self-Service Portals for health eligibility and selection of programs. Completing the requirements for FISMA certification for an organization which enabled them to win a ing $75million dollar multi-year contract with Veterans Administration (VA) in their Healthcare Benefit program for Veterans. Consulting roles/client as Independent Consultant as follows: Sabbatical February 2017 to January 2018 Senior Security Engineer Consultant IBM - Pittsburgh, PA April 2015 to February 2017 Works remotely with Internal Key Controls over Operations (KCO) Performed Risk Assessment and 27001/2 gap analysis on company's global application, network, and external cloud service provider. Assisted the Information Risk Management (IRM) team in the re-design of Vendor Risk Management (VRM) compliance process and procedures. Provided consultative support in the development of ISO 27001 Certification roadmap to include all region and global locations. Provided consultative guidance on implementing GRC solution for performing Vendor Risk Assessments. Developed cross-reference matrix of regulatory controls to minimize efforts for building 3rd party risk assessments that were ported to Archer. Assisted in the selection of monitoring and auditing tools to satisfy semi-annual and annual requirements of vulnerability testing and reports for company's clients and customers. Senior Security Engineer Consultant BNY Mellon - Pittsburgh, PA October 2014 to March 2015 Performed Risk Assessment and 27001/2 gap analysis on company's global application, network, and external cloud service provider. Assisted the Information Risk Management (IRM) team in the re-design of Vendor Risk Management (VRM) compliance process and procedures. Provided consultative support in the development of ISO 27001 Certification roadmap to include all region and global locations. Performed and led the Third-Party Vendor assessments to validate SOX controls are effective. Provided consultative guidance on implementing GRC solution for performing Vendor Risk Assessments. Assisted in developing assessment templates to import Shared Assessment Control Libraries into Archer. Assisted in the

selection of monitoring and auditing tools to satisfy semi-annual and annual requirements of vulnerability testing and reports for company's clients and customers. Senior Security Advisor Indonesia Office - Pittsburgh, PA July 2013 to September 2014 Developed and supported implementation of new office for Information Security Services located in Pittsburgh, PA and Jakarta, Indonesia (Asia). Performed Risk Assessment and 27001 compliances on company's internal network systems and external cloud service provider in both USA and Indonesia. Provided solution and deployment plans for IAM and UOM requirements for various minister and government agencies to support provisioning and de-provisioning of controlled access. Developed policies and procedures for maintaining compliance and auditing requirements following the government security requirements as listed in ISO 27001:2005; FISMA; PCI-DSS for US office and Indonesian Regulation 82 for ASEAN data protection Wrote all internal company Information Security policies to include third-party vendor management policies and integrated governmental Information Assurance (IA) requirements to satisfy statement of work (SOW). Assisted in the selection of monitoring and auditing tools to satisfy semi-annual and annual requirements of vulnerability testing and reports for company's clients and customers. Proof-point Systems - Los Altos, CA May 2012 to July 2013 Performed Risk Assessment on company's outsourced cloud infrastructure to prepare them for contract services with DOD agency. Developed policies and procedures for maintaining compliance and auditing requirements following the government security requirements as listed in FISMA. Developed and wrote Information System Security Plan for proprietary software application that DOD would use for gathering sensitive data. Conducted Gap Analysis on company's outsourced cloud service to identify controls that were not in compliance with regulatory requirements under the Federal Information Security Management Act of 2002. Wrote Plan of Action and Milestone (POA&M) to implement necessary controls to mitigate those gaps addressed during assessment. Wrote all internal company Information Security policies to include third-party vendor management policies and integrated governmental Information Assurance (IA) requirements to satisfy statement of work (SOW). Assisted in the selection of monitoring and auditing tools to satisfy semi-annual and annual requirements of vulnerability testing and reports. Wrote

Information Security Appendix for DOD Statement of Work (SOW) that Proof-Point Systems would perform software application services for. Created documentation and road-map architectural drawings for company's outsourced data center to become Fed RAMP compliant. Provided Certification and Accreditation (C&A) advisory support and developed all documentation for presenting C&A package to Defense Security Services (DSS) Performed duties as Interim Chief Information Security Officer (CISO) during the time on contract and assisted in hiring and transitioning responsibilities to new CISO. Security Architect Harmonized Security and Privacy Framework - Topeka, KS January 2012 to May 2012 Developed Risk and Compliance processes for the integration of healthcare systems from one outsourced provider to another outsourced provider's technology platform. Identity, Credential, and Access Management (ICAM) - Oracle's COTS Identify Management solution was selected for identity proofing, authorization and authentication. The Enforcement and Eligibility project incorporated the principles which are currently addressed in the Harmonized Security and Privacy Framework. Major responsibilities were to ensure all security-related requirements were properly reviewed and accepted into the requirements management matrix; this included derived requirements. Assisted in the collection of security issues in the secure Infrastructure of cloud computing; the State of Kansas project will have a multi-zone architecture to ensure the solution had the capability to be used by additional states; this architecture extended to my role as security handler. Confirmed baseline and specific requirements of Oracle's IAM 11g, for the Self-Service Portal project were entered into the design documents and they adhered to all applicable federal and state security standards. Assisted the State in the requirements gathering, analysis, design, development, and testing of the deployment and application support of Oracle's Identity and Access Management implemented between several different agencies of the state. Analyzed industry "best practices" which were or were not being followed during other State implementation(s) of Accenture's Public Service Platform (APSP) which is built Service-Oriented Architecture (SOA) principles and methodologies. The APSP uses Oracle's Enterprise Application Suite, including the Oracle Access Manager. OAM was an integral part of the overall cross domain SSO and federated services. Ensured the migration from Sun Identity to the

Oracle IAM solution component met all security requirements defined during the design phase. Emphasis for this evolved around application security, including authentication, authorization, role-based access control (RBAC) to include extended RBAC (groups, privileges), credential mapping, encryption and certification and keys. Assisted in development of plans for the System and User Acceptance Testing (UAT) Develop security-related testing plans including test scripts. The UAT plans were developed to ensure all security and identity management functionality and interfaces were thoroughly tested end-to-end to ensure there were no unacceptable vulnerabilities in the solution. Assisted State and contractor staff in the performance of Risk Assessment and Security Plan and System Security Plan (SSP) per CMS and Federal/State requirements. Utilized NIST SP 800 series for guidelines. Wrote and published for State approval; policies and procedures for managing and authorizing changes to APSP Oracle's IAM security profiles and assigning profiles to users. Oversaw major security and privacy controls and capabilities of the Accenture APSP solution across each phase of the project lifecycle. J.D. Power and Associates - Thousand Oaks, CA May 2011 to January 2012 Developed Risk and Compliance processes for the integration of healthcare systems from one outsourced provider to another outsourced providers technology platform. Provided consultative support in the development of ISO 27001 Certification roadmap to include all region and global locations. Performed Self-Assessment of agency's security environment and developed road-map to remediate risks and establish acceptable mitigating processes. Performed FISMA assessments in accordance with NIST 800 series. Developed road-map for State Agencies to meet the requirements of HIPPA, HITECH and the Federal Information Security Management Act (FISMA) of 2002. Medi-Cal - Sacramento, CA March 2011 to May 2011 Developed Risk and Compliance processes for the integration of healthcare systems from one outsourced provider to another outsourced provider's technology platform. Performed Self-Assessment of agency's security environment and developed road-map to remediate risks and establish acceptable mitigating processes. Performed FISMA assessments in accordance with NIST 800 series. Created Security Architect design roadmap for migrating access control requirements from outsourced provider using Sun Identity Access Management platform to

the States new IAM which was comprised of several federated service solutions and Oracles Identity Access Management 10g. Developed road-map for State Agency to meet the requirements of HIPPA, HITECH and the Federal Information Security Management Act (FISMA) of 2002. Financial Industry Regulatory Agency - Rockville, MD April 2010 to March 2011 Developed Risk and Compliance processes for management of Vendor organizations to include Offshore Data Center risk and compliance assessment using ISO 27001-2005. Performed Self-Assessment of agency's PCI-DSS environment and developed road-map to remediate risks and establish acceptable mitigating processes. Integrating IT Policies, Standards, and Guidelines into automated processes using RSA Archers IT risk, compliance, incident, and policy tools within the RSA eGRC, as well as cross-utilization with Internal Audits tool, Protiviti. Provides guidance on securing Federal Systems that FINRA uses to work with Federal Government Agencies in meeting their business requirements. Performed FISMA assessments in accordance with NIST 800 series. Freddie Mac - McLean, VA January 2010 to April 2010 Assisted the Freddie Mac Risk and Compliance team in analyzing over 500 application systems for risks and vulnerabilities using ISO 27001-2005: Provided oversight in risk assessment process re-engineering to ensure cost effectiveness. Assisted in the development of a process framework for the implementation and management of controls to ensure that the specific security objectives of Freddie Mac were met. Catholic Healthcare West - Phoenix, AZ December 2008 to June 2009 Provided senior management duties to 8th largest Health Care Institution in the United States. Duties included the following: Provided management oversight on access-controlled activities of various operating systems, servers, and software. Provided superior administration tasks such as configuration, user management, patching, and log management, using Oracle Access Manager (OAM) and Oracle Internet Directory (OID) enabled the IAM team to assist with troubleshooting and updates. Overseen a network of security managers and vendors who safeguard the company's assets, intellectual property and financial accounting systems, as well as the physical safety of employees and visitors. Provided management responsibilities for 37 Information Security Analysts, Engineers, Administration and Risk and Management personnel to include quarterly reviews, training assignments, and related

management responsibilities. Implemented process and procedures for segmenting global network to support PCI-DSS requirements of all hospital, clinical, and pharmacy locations through-out the three state area of Arizona, California, and Nevada. Included integrating security help desk located in India Developed and implemented risk-based process for performing security assessment and reviews of all critical systems that supported regulatory requirements of HIPAA, Sarbanes-Oxley, and PCI-DSS. Assisted application teams in building security road-map for the re-design of web-based portals from Novell's Identity Management solution to Sun Identity Management. Built audit and compliance review tests for the migration of Novell Identity Management to a java based web-services solution. Coordinated the development, implementation, and administration of Catholic Healthcare West security policies, standards, and guidelines for all 40 hospitals and over 200 clinics. Implemented an automated solution (PolicyIQ) to migrate security policies and standards from hard copy to electronic copies. This enabled a work-flow process that ensured all departments and interested personnel reviewed/approved all policies and standards. Managed administration and implementation of application and system monitoring using NetIQ security manager. Implemented security management and monitoring across enterprise from centralized location, reducing resourcing costs for remote locations. Bank of America September 2008 to December 2008 Provided senior security analyst duties to Bank of America during integration with Countrywide Financial Corporation as a subcontractor with Ajilon. Duties included the following: Provided information security control oversight on access-controlled activities during the integration of financial systems between the two organizations. Provided risk assessment support on new systems that were developed and implemented during the migration. Created data-base design for the collection of all financial and non-financial systems to provide prioritization of critical systems for implementation in Disaster Recovery and Business Continuity programs. Reviewed new system designs for financial system support to ensure controls were implemented and designed to support necessary regulatory requirements. Catholic Healthcare West May 2008 to September 2008 Provided senior management duties to 8th largest Health Care Institution in the United States as a sub-contractor with Perot Systems. Duties included the

following: Provided management oversight on access controlled activities of various operating systems, servers, and software. Provided management responsibilities for 37 Information Security Analysts, Engineers, Administration and Risk and Management personnel to include quarterly reviews, training assignments, and related management responsibilities. Implemented process and procedures for segmented network to support PCI-DSS requirements of all hospital, clinical, and pharmacy locations through-out the three-state area of Arizona, California, and Nevada. Developed and implemented risk-based process for performing security assessment and reviews of all critical systems that supported regulatory requirements of HIPAA, Sarbanes-Oxley, and PCI-DSS. Coordinated the development, implementation, and administration of Catholic Healthcare West security policies, standards, and guidelines for all 40 hospitals and over 200 clinics.

Implemented an automated solution (Policy IQ) to migrate security policies and standards from hard copy to electronic copies. This enabled a work-flow process that ensured all departments and interested personnel reviewed/approved all policies and standards. Senior Information Systems Administrator for the Enterprise Information Management department Wells Fargo Bank September 2006 to January 2007 09/2006 to 01/2007 Provided senior information security consultant duties in a financial environment. Duties included the following: Administered and controlled activities of various operating systems, servers, and applications that supported all financial services areas of the bank. Hardware supported and serviced included (PC&/or Mainframe) PC and Server operating systems include; Windows XP, Windows Server 2003 Servers Operating Systems Used: Windows XP, Windows Server 2003 Performed and lead systems administrators in general direction, installation, maintenance, and the configuration of various operating systems, servers, desktops and various application software. Performed problem management support through troubleshooting various components of the network through the use of various industry NMS tools. Additionally, programmed and analyzed various information systems. Worked with internal and external clients to resolve hardware, software, and systems issues. Evaluated systems specifications and installation parameters. Assisted in the implementation of systems and software enhancements to improve the reliability and performance of systems. Assisted in evaluation of

new systems software and hardware. Provided assistance and performed duties that included the development of tools to manage systems and make all services available to users. Performed and conducted security assessments, reviews, and worked with internal and external audit agencies to meet regulatory requirements. Installed and managed Anti-virus and email spamming solutions for enterprise and resolved end-user problems with installation of security software. Senior Information Systems Administrator for the Enterprise Information Management department. Conducted risk management reviews of organizational financial systems. Provided oversight and security plan development for financial services lines of business, to include wholesale services, retail banking, lending and mortgage lines. Designed and Implemented Secure Network Architecture between various business lines to include separation of non-public and public information on separate networks. Assisted Information Security department in reviewing and updating approximately 1200 network system, operating procedures, and security plans. IT SOX Project Lead AIG February 2004 to September 2006 02/2004 to 09/2006 Provided senior information security consultant duties in a financial environment and airlines organization. Duties for both contracts included the following: IT SOX Project Lead for a financial services organization that included banking, mortgage operation services and retail leasing services. Managed and supervised up to 10 Security Risk Analysts during the time of the project. Developed and implemented an IT SOX methodology to include, a Risk Assessment process to simplify the identity of high-risk systems that were applicable for inclusion in the overall SOX project. Assisted Internal Audit in developing the overall scope and plan for implementation and completion of IT SOX requirements at five company locations, located in the southeast. Performed Lead Systems Administration with IT department to ensure that systems were built, configured and secure for the entire enterprise Conducted interviews for additional IT auditors to assist in the documentation, remediation, testing, and re-remediation at the five designated company locations and assisted those auditors in the ramp up for performing IT SOX duties at these locations. Assisted in the documentation phase to complete all process documentation under a very aggressive timeline and successfully completed 96% of all process narrative documentation in six short weeks. Assisted in

the development of test plans for all key IT controls that was determined by management as being key processes for reporting of financial information. Systems include AS400s UNIX, Windows, and IBM mainframe operating systems utilizing Z/OS with ACF2 and RACF. Performed problem management support through troubleshooting various components of the network through the use of various industry NMS tools. Provide systems administration guidance in working with Internal and external auditors to review and assess third party organizations that performed IT functions that involved processes for the organization that involved those reports that dealt with financial reporting. This included reviewing SAS70 Type II reports to ensure the period of testing would be covered as required by SOX regulations. Information Security and Financial Review Services January 2003 to February 2004 Provided partners and management staff with Chief Security Officer Responsibilities during the start-up phase for an Information Security and Financial Review Services company. Duties included the following: Assisted financial organizations and higher education with establishing and maintaining an effective information system network; a secure framework, and effective and secure architecture that provided assurance that business-wide information system operations and security strategies are aligned with business objectives and that critical data is was stored and transmitted effectively, efficiently, and secure. Developed and implemented methodologies for clients to identify and manage information security risks. Oversaw clients application development Provided a team of highly experienced security analysts to clients to assist in the design and development of effective information security programs that implements information security governance frameworks. Conducted Risk Assessments and developed effective Business Resumption program plans Performed RACF/ACF2 Administrative responsibilities to numerous financial and service-oriented organizations. Provided Systems Administration duties that included the building of a Windows environment built on Windows 2003 Server technology. Implemented and deployed application software to all end users and provided in-house training and problem solution to the entire enterprises, bank wide. Provided implantation services for Sarbanes-Oxley compliance requirements, Graham Leach-Bliley Privacy Issues and other regulated requirements. Chief Information Security Officer (CISO), MUTUAL OF NEW YORK

(MONY) - Syracuse, NY 2001 to 2003 Director, Information Security Compliance, ACXIOM CORPORATION - Little Rock, AR 1999 to 2001 Chief, Information Security USAF (CIVILIAN) - Warner Robins, GA 1992 to 1999 Education Bachelor of Science in Information Security AMERICAN MILITARY UNIVERSITY Associate Degree in management Information Systems COMMUNITY COLLEGE OF THE AIR FORCE (CCAF) - Warner Robins, GA Skills auditing (10+ years), Risk management (4 years), Security (10+ years), solutions (10+ years), It Audit, Fisma, SOX, Cobit, Cisa, Compliance, CIA, Hipaa, Nist Military Service Branch: United States Air Force Rank: E-9

Name: Anthony Robinson

Email: dylanwilliams@example.org

Phone: 001-543-348-6839