

IT COMPLIANCE AUDITOR, PCI DSS, GRC IIS/ INSIGHT GLOBAL (CONSULTANT) IT COMPLIANCE AUDITOR, PCI DSS, GRC IIS/ INSIGHT GLOBAL (CONSULTANT) IT SUPPORT SPECIALIST Odenton, MD Over 12 plus years of fulltime consulting in Information Technology. I whole-heartedly possess a positive support and service attitude when working with all projects. I strongly believe in being a team player with ability to adapt to changes. Known for efficiently managing complex and varied workloads, setting appropriate priorities with the ability to work under pressure, even with frequent job-related interruptions that can frequently happen. Highly detail oriented and organized, with ability to anticipate needs before they surface. Ability to work across organizational boundaries to obtain information and accomplish goals. Willing to assume responsibility for and follow through on independent projects. Ability to handle sensitive information to ensure confidentiality. Ability to communicate and interact tactfully and effectively with discretion.

CORE COMPETENCES 12 years of IT Technical Support. 10 years Subject Matter Expert for Cyber Security 10 years proficiency in PMP Technical Support Specialist. High proficiency in software, database, implementation, configuration, migration, integration and application technologies. Ability to multitask in a fast-paced high volume environment. CORE TECHNICAL SKILL SETS: IT Security PMP Integration Migration UNIX/LINUX Windows OS TCP/IP DNS/DHCP WAN/LAN VLAN VPN Servers 2003-2010 NTFS RDP Microsoft Project Microsoft Suites SDLC Remote Access RSA Citrix Cisco SIEMS Active Directory Windows Anti-Virus Malware IDS/IPS SCCM Mobile phones ITIL Remedy JIRA Service Manager Symantec DLP LogRhythm Cisco Nmap Nessus Splunk Identity Access Management SOX PCI/DSS Authorized to work in the US for any employer Work Experience IT COMPLIANCE AUDITOR, PCI DSS, GRC IIS/ INSIGHT GLOBAL (CONSULTANT) COMCAST - PHILADELPHIA HEDQUARTERS July 2016 to May 2017 Championed internal control and corporate governance concepts for PCI DSS. Travel 35% of the time assessing Payment Center , Xfinity Stores, Call Centers, Data Centers and Divisional HQ for PCI DSS. Responsible for assessing the development and implementation of effective and reasonable policies and practices for PCI-DSS to secure protected and sensitive data and ensure information security and compliance with relevance. Responsible for the auditor efforts

to internally assess, evaluate and make recommendations to management regarding the adequacy of the security controls for the company's information and technology systems for PCI-DSS.

Worked with Internal Audit, External Auditors and outside consultants as appropriate on required security assessments and audits for PCI-DSS. Coordinated efforts and tracked all information technology and security related PCI DSS audits including scope of PCI-DSS audits, Comcast payment stores involving, timelines, auditing agencies and outcomes. Worked in association with PwC auditors to appropriate audit focus in scope and maintain excellent relationships with audit entities. Responsible for PCI scope management, including defining PCI scope. (understanding PCI segmentation and demarcation environment). Evaluated the need for continuous monitoring and compliance of controls, including responses to out of compliance situations and remediation approaches. Acted as the directed point of contact to assist with the completion of the PCI DSS SAQ templates and manage the PCI Manager Portal. Developed a knowledge-base/FAQs to answer commonly asked questions related to SAQ completion. Provided direct support to answer any questions related to the SAQs. Worked with leadership and relevant responsible compliance department leadership to build cohesive security and compliance program for Comcast to effectively address global statutory and regulatory requirements of PCI-DSS and the building of the ROC (Report On Compliance) Finalized the completion of the 2017 ROC by incorporating PCI-DSS into a holistic governance, risk and compliance (GRC) program at Comcast Headquarters in Philadelphia.

Developed a strategy for dealing with increasing number of audits, compliance checks and external assessment processes for internal/external auditors, PCI-DSS, FCPA and SOX. IT Security Architect Lead/ Paragon Solutions (Consultant) CSL Berhring Pharmaceuticals - King of Prussia, PA September 2014 to July 2016 This position supported the Greenfield project with overall information security infrastructure for Seqirus. Seqirus is a newly formed Pharmaceutical/ vaccine company, which was formally Novartis. As an IT Security Lead Architect for the Infrastructure integration technology REDIT/EDGE team. I was responsible for the build of IT Physical Security ITIL strategies defining, deploying, monitoring and maintaining physical security, IT security architecture, infrastructure platforms, application security, tools for the startup of the administration/management

and related business processes and workflows structures. Managed the coordination and implementation of endpoint protection technology products and solutions. Managing all parts of incident, change, request and problem management. Completely managed the continuous management and monitoring of software, analyzing and remediation of security incidents and alerts. Produced a Forward schedule of change and CAB reports. Also was accountable for various 3 party vendor selections as well as writing Request for Proposal (RFP), Request for Information (RFI), Request for Quotation (RFQ). Created a problem management catalogue to track and identify trends. Provided timely updates to key delivery and customer stakeholders on the status of any major incidents. Reduced the average Key performance indicators (KPI) performing security and for budget, Capital Approval Request (CAR). QA practices related to 21 CFR Part 11 Compliance security projects this is a firm posture and overall responsible for the protection of all Information Technology assets in Seqirus pharma. IT Security Analyst RevSpring Inc - Oaks, PA December 2012 to August 2014 Implemented the infrastructure components supporting emerging technologies and applications. Performed IT Audit and compliance, SSAE16 SOC1Type II/SAS 70 Type II. Responsible for analyzing PCI-DSS assessment findings, owner identification, remediation planning and validation. Worked with all IT functional groups to insure all PCI compliance requirements, such as Internal PCI Scans, External PCI Scans, PCI Segment Network documentation, were executed in a timely manner as required by the PCI-DSS standards. Prepared activity and progress reports ensuring issues are properly escalated and resolved to maintain delivery schedule, project cost, and desired results; provide actionable after-incident analysis to ensure root cause issues are logged and remediated compliance. Developed and maintained skill proficiency in PC-based operating systems. Tested, scanned and troubleshoot local area networks (LANs), wide area networks (WANs), and Internet systems for any issues or targeted back door assaults. Installed network hardware and software and make needed upgrades and repairs. Performed isolated design software installs, testing and operational verification prior to design software implementation to the department and engineering consulting firms. Tested new CADD and engineering software releases, updates or program fixes for compatibility with current procedures and hardware configurations.

Troubleshoot network connectivity and hardware issues and escalates problems that cannot be appropriately resolved. Resolved issues with Microsoft Exchange 2003/2008/2010 Server and Outlook clients. Provided customer service for defense electronics products and systems. Received calls and emails from customers and field support personnel. Addressed hardware, software and other issues for company products and systems. Generated service tickets and route to appropriate departments/individuals for resolution. Maintained help desk database and service history. Developed and utilized in-depth understanding of products/systems to directly assist customers with setup, operation and troubleshooting. Coordinated returns and equipment exchanges. Interface with company personnel to resolve issues. Documented processes and procedures. Experienced with defense electronics, both hardware and software, required. Hardware/software troubleshooting skills, understanding of network concepts and Windows/Linux highly desirable. Experienced with JIRA Service desk desirable. Network Security Administrator firstPRO Philadelphia, LLC - Moorestown, NJ November 2010 to November 2012 Responsible for maintaining access control within regional or contractual standards for IT Security Interface with Information Technology ( IT) and National Security Engineering Operations) Maintain workstations and laptop computers including systems in industrial environments. Deployed and configured user workstations and accessories per on-boarding requirements. Order replacement consumables, as necessary, by contacting various vendors for purchases. Troubleshoot, installed, and configured network printers. Performed initial troubleshooting on all break-fix tickets as a tier 2 support assisting in NOC/HD Monitored and configured security systems, including but not limited to IPS, VPN, SIEM and netflows, in order to protect the Comcast network from malicious activity and to identify compromise. Configured, joined to domain, updated, troubleshot, repaired and upgraded all computers within the 1180+ user environment. Created and updated Ghost base images of machines for easy OS (re)installs. Set up RSA accounts. (IBM), business users and technical support teams Intuit 2012 to 2012 Configured, updated, and supported many popular software applications based on Microsoft (XP/Win7 OSs as well as MS Office 03/07/10/365), Intuit (QuickBooks Ent. 2012), PeopleSoft (Fast and GEMS) and Adobe (Acrobat & Creative) platforms.

Worked closely with the 3rd party vendor (IBM), business users and technical support teams for the migration of technical support duties. Supported key Information Security technologies, such as SIEM, DLP, Vulnerability Management. Aided and ensuring hardware/software compatibility; and coordinated and/or modified user requirements in terms of existing and projected computer capacity and capabilities. Provided assistance as in-house helpdesk and technical support by phone and in person to facilities staff. Assisted with the installation of computer systems on site and for existing and new customers to include maintenance and IMAC requirements. Performed upgrades on existing computer systems to include server 2003, 2008 Monitored Peregrine Service Center and updated system as work was completed. IT Security Officer About Consulting LLC - Chadds Ford, PA November 2008 to November 2010 Acted as a hands-on technical resource for the AZ IT Security GSM IT Security team globally. UNIX and Linux environment. Handled multiple projects and deadlines in a timely manner for BAU process. Coordinated access request with offshore areas of AZ IT Security IBM/ Bangalore support (Help- Desk). Senior IT Security Analyst TekSystems - Radnor, PA October 2007 to October 2008 Was responsible for the Re-modification, development and deployment of the in-house Identity Management, Web based system, called System Access Request (SAR). A multi departmental security profile web-based identity access management system for Help Desk Security and Standards. Enhanced efficiency and decreased downtime by 25% for 300+ networks and 3100+ machines. Improved user productivity by up to 50% via scripting, troubleshooting and repair methods. UNIX Administrator Accenture - Philadelphia, PA January 2007 to October 2007 Was responsible for writing and the implementation of DuPont's technical Infrastructure and LDAP security bylaws for the UNIX/Linux environment. As well as the development and implementation of the architectural design for the National Operational Standards for Technical Security documentation of Help Desk Tier level standards. Assisted multifaceted crowd of users from different contracts with all technology related issues., 25-40 average tickets per day. Remotely connected to users computers using LANDesk, Microsoft IM or NetMeeting, 95% issues resolved at first contact. IT Security Administrator Accenture - Philadelphia, PA May 2006 to January 2007 Was the technical advisor for the migration and conversion of SAM ( Security Access

Manager). The access management monitoring system for CA- Identity Management Suite Management and CA-Administration Manager, for Vanguard's Business Access Management (BAM). Ensured that changes are recorded and that authorized changes were prioritized, planned, tested, implemented documented and reviewed in a controlled manner. Manage Active Directory network, which involves creating and modifying accounts and groups, modifying group memberships, establishing permissions, resetting passwords, and ensuring proper access to network resources such as mailboxes, file shares and printers. Performed desktop and laptop imaging including hard drive recovery utilizing the recovery backup process for data retention. Troubleshooted and resolved Virtual Private Network (VPN)/SSL, RDP connectivity issues for remote users. Inspected employee equipment and software periodically for adequate functionality including patches and updates Computer Systems Specialist Computer Associates International Inc - Princeton, NJ July 2005 to May 2006 Was the Third-level, technical support and analytical problem solving and management to end users on complex issues regarding RACF/Mainframe, VMS, AS400 and server operations, including setups, error messages, on-line transactions, system status and downtime procedures for the product use of eTrust CA-7 Top Secret Security. IT Security Administrator/ Kelly IT Services Cooper University Hospital - Mount Laurel, NJ May 2004 to July 2005 Mount Laurel, NJ May 2004 to July 2005 Technical responsibilities include: Full roll-out of Active Directory in UNIX/Linux environment responsible for the migration of CUH users and devices from the multiple existing legacy NT domains, to Windows 2003 Active Directory Domains in hospital and satellite offices. 3rd level technical support for CUH; in-house, remote users as well as 3rd party vendors. Investigated and resolved security incidents using Symantec AV logs. IT Security Administrator/ Kelly IT Services, Radnor, PA/ Campbell Soup Company, Camden NJ IT Security Administrator Kelly IT Services/ Campbell Soup Company - Radnor, PA July 2002 to April 2004 Responsible for the Technical support and security of the Active directory. Responsible for the updating and the installations of AV on all servers. Responsible for the provisioning and modification of Novell user accounts. Analyzed, resolved and documented reported incidents. Maintained the Active Directory structure and all interrelated authentication systems, including the administration of

user accounts, shared resources and access permissions. Distribute hard and soft key fobs for RSA accounts. Technical Support Unisys January 2000 to June 2002 AS400 and Tivoli FRB Data Center; UNIX/Linux environment. Logged and supported calls through Tuxedo system. 45% Technical Support, 55% Systems Operator. Resolved 90% of customer problems while they were on the telephone and email. Created user accounts and power passwords for system. Ran scheduled batch process. Provided shell scripts to retrieve and manage data. 3rd Shift Computer Operator/Anchor International State Lottery - Sharon Hill, PA July 1994 to January 2000 Teir II technical Help Desk support configuration, transport, deployment, performance, maintenance, testing, architecture, security, monitoring of data center in UNIX environment. Technical phone support for internal helpdesk. Education Associates Degree in Computer Electronics Technology Computer Learning Center - Plymouth Meeting, PA 1997 Skills IT Compliance (10+ years), Process Safety Management (6 years), Microsoft Suite (10+ years), Remote Access (10+ years), RDP (7 years), UNIX/LINUX (10+ years), PCI DSS (6 years), CISCO (10+ years), VPN (10+ years), SOX (10+ years), TCP/IP (10+ years), LDAP (8 years), Citrix (6 years), NTFS (9 years), Active Directory (10+ years), RSA (8 years), IDS/IPS (9 years), WAN/LAN (10+ years), System Administration (10+ years), SQL (8 years), SIEMS (8 years), Symantec (10+ years), Windows Servers (10+ years), Anti virus/Malware (10+ years), VLAN (9 years), DNS (10+ years), Dhcp (10+ years), JIRA (5 years), Remedy (7 years), Splunk (5 years), IT Security (10+ years), NMAP (7 years), Nessus (9 years), NOC (4 years), Asset Protection (10+ years), Compliance (10+ years) Links <http://WWW.LINKEDIN.COM/IN/WANDA-MONTAGUE-32062211> Certifications/Licenses MCPS: Microsoft Certified Professional April 1997 to Present ITIL July 2011 to Present Cisco Certified Network Professional (CCNP) March 2007 to Present CISSP October 2013 to October 2017 Inactive A+ Certified April 1998 to Present Additional Information CORE COMPETENCY 12+ years of hands on IT Technical Support. Subject Matter Expert for Cyber Security 11 years proficiency in Technical Support High proficiency in software, database, implementation, configuration and application technologies. Ability to multitask in a fast-paced & high volume.

Name: Frank Walker

Email: bwebster@example.com

Phone: +1-404-906-0059x13102