IT Auditor IT Auditor Greensboro, NC IT Audit professional with years of experience in both IT consulting and corporate internal Audit. Strong experience in the planning and execution of internal audit procedures over SOX compliance and collaborating with external auditors to increase the reliance rates. Strong understanding of the IT General Controls over IT Operations, Access, Security, Change management and Backup procedures. Knowledge of ITIL incident, problem & change management. Performed risk assessment for various IT Audit projects utilizing frameworks and standards such as 27001 and COBIT. Several years experience in Desktop Support, IT Security, System Administration, Server Deployment and Configuration and IT Auditing. Proven ability to troubleshoot and resolve hardware, software, and mobile device issues. Extensive experience in developing procedures, policies, technical manuals, software guides and instructions, executive briefings and presentations. Proficient with Windows platforms, MS Office and Computer systems repair and maintenance Vast experience in auditing security solutions such as Data Loss Prevention (DLP), Enterprise Fraud Management (EFM), Vulnerability Assessment, Security Information & Event Management (SIEM), Unified threat Management (UTM) and Endpoint Security as well as reviewing firewall rules. Vast experience in business continuity and IT Asset Management tools. Authorized to work in the US for any employer Work Experience IT Auditor The HCI Group January 2017 to Present Perform PCI DSS, HIPAA testing at doctors' offices, hospitals and health insurance providers. Evaluated sufficiency of employee education material regarding social engineering threats and phishing attacks. Reviewed security configurations around server and database platforms Performed disaster recovery and business impact analysis Conducted audit readiness with the aim of reducing controls weaknesses. Assessed the adequacy and coordinated the implementation of specific information security controls for new systems and services. Reviewed documented information security policies, standards and procedures. Execute information security audit, testing preventative, corrective, detective and compensating controls. Conduct semi-annual access review for all applications especially those with financial impact on the organization. Responsible for performing internal audit assignments as defined in the internal audit plan, also assist with special projects and management assigned tasks Execute

information systems audits which includes ITGCs testing, IT Application Controls testing and IT Infrastructure audit including, but not limited to Active Directory, Operating System, Servers, Network Device and databases. Review SOC 1 type 2, perform SOC 1, 2 and 3 evaluations. Test PCI DSS controls for design appropriateness and operating effectiveness. Participate in new systems development and post implementation audits to ensure the System Development Life Cycle (SDLC) is followed and to ensure adequate internal controls are built into the system Responsible for identifying, evaluating and documenting key IT risks and controls throughout the organization, across multiple information technology platforms Develop and implement process for ongoing monitoring of IT processes to ensure compliance with SOX audit controls. Maintain and update the remediation tracker to follow-up on the status of outstanding internal audit findings Participate in all phases of internal audit assignments including planning, execution, reporting and follow up IT Auditor Fasyl Technology Group May 2014 to December 2016 Participated in disaster recovery procedures across Windows, O/S, UNIX and other infrastructure audit. Plan and execute Information Technology Audit. Ensure audit tasks are completed accurately in a timely manner engaging COBIT, COSO, and ITIL frameworks. Performed ITGCs and application controls testing internally for the company. Perform information security audit; testing preventive, corrective, detective and compensating control for design appropriateness and operating effectiveness. Perform special projects and technical audits, such as IT infrastructure testing of servers, firewalls, databases, operating systems and network services. Keep Senior Management and Auditees abreast of identified IT Audit findings. Perform SOX Compliance Audit, challenging IT projects, PCI DSS, HIPAA, Data Center Audit, and identify conflicts or inadequate internal controls and issue recommendations. Perform annual SOX Compliance testing of primary controls ITGCs and IT Application controls using COSO and CobiT frameworks and other industry best practices standards. Possess working knowledge of SSAE18 and GDPR regulation. Perform walkthrough and testing to determine company compliance on assigned SOX processes and documents testing results and communicate results to the process owners. Execute information security audit, testing preventative, corrective, detective and compensating controls. Conduct semi-annual access

review for all applications especially those with financial impact on the organization. Responsible for performing internal audit assignments as defined in the internal audit plan, also assist with special projects and management assigned tasks. IT Security & Systems Administrator Fasyl Technology Group March 2012 to April 2014 Active Directory, Office 365 and Google Apps Administration. Firewall Administration. Develop and maintain installation and configuration procedures Apply OS patches and upgrades on a regular basis. Configure and support security tools such as Firewalls, Anti-virus software, Unified Threat Management (UTM), Vulnerability and Patch management software (GFI LanGuard). Fortinet Administration and support. Offering pre-sales support to sales reps and agents (Hardware and Software upgrades) Perform daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems and key processes, reviewing system and application logs. Installation and support of SAGE ERP server. Implementation of Enterprise Fraud Management (EFM) Solutions for Banks. IT Security Analyst Electronic Payplus Limited January 2011 to January 2012 Windows Active Directory administration. Assigning and maintaining user logon and access privileges on the server. Account creation and Password reset for Banks on the EFT and FTP server. Installation and user account administration on the EFT, FTP, KMS and Data preparation Server. Maintaining, configuration and monitoring of the Syslog and the Anti-virus server. Updating and managing the company website. Experience of using System Administration tools such as Hyena Scanning the network to check for vulnerabilities using GFI LanGuard. Quarterly review of the network documentations and policies. Investigate user problems, identified their source, determine possible solutions, test and implement solutions. Install, configure, and maintained personal computers, workstations, file servers, Ethernet networks, network cabling, and other related equipment, devices, and systems Physical verification of IT assets in conjunction with IAC department and CISO. Review critical patch updates for vulnerability before updating the patch on all critical systems on a weekly basis. Closure of audit non-conformities within stipulated time (Verve, MasterCard, VISA and internal audit) Monthly independent checks of network devices, user accounts, and permission level of critical business machines in conjunction with the CISO.

Education Bachelor's January 2004 to August 2008 Diploma in Network Security and Server Administration Zoom Technologies March 2009 Skills IT Service Management (7 years), ITIL (7 years), Microsoft Project (2 years), IT Audit (4 years), IT Security (8 years), System Administration (8 years), IT Support (8 years), security, Active Directory, training, Cisa, SOX, Auditing, Compliance Certifications/Licenses ITIL Foundation in IT Service Management (ITIL v3) March 2012 to Present License # 4463769.1069920 MCP: Microsoft Certified Professional April 2012 to Present License # E909-6597 Microsoft Certified Solutions Associate (MCSA): Windows Server 2008 April 2012 to Present License # D717-9401 Microsoft Certified IT Professional (MCITP): Server Administrator on Windows Server 2008 May 2009 to Present License # D074-3962 Microsoft Certified Technology Specialist(MCTS): Windows Server Active Directory Configuration May 2009 to Present License # D074-3960 Microsoft Certified Technology Specialist (MCTS): Windows Server 2008 Network Infrastructure May 2009 to Present License # D074-3961 Symantec Endpoint Protection 12.1 (SEP) March 2013 to Present Symantec Data Loss Prevention (DLP) May 2013 to Present Symantec Backup Exec. Cloud 2013 (BE.Cloud) June 2013 to Present Symantec Backup Exec 2012 (BE) March 2013 to Present

Name: Christopher Green

Email: tiffanybrown@example.org

Phone: 869-805-9954x663