

Information System Security Officer (ISSO) Information System Security Officer (ISSO) Information System Security Officer (ISSO) - Baxter International Inc Charlotte, NC A highly motivated individual, dependable professional with great communication attributes. Skilled Information Security Analyst with expertise in risk management, security control selection, Host based intrusion detection and prevention, and various vulnerability management tools. Looking for a position within the Information and Cybersecurity Field. I have a total of 3 years professional experience in the IT field working as a security analyst. I have participated in security assessment based on NIST 800-53A, 800-39 800-137 800-115 FIP 199 and 200. Apart from the above I've volunteered also as an IT instructor mentoring student after hours and on weekends. My goal is to be an effective team member contributing to the development of the corporate environment and my team. Fluently communicate in English and French. Active military (U.S Army Reserve). Work Experience Information System Security Officer (ISSO) Baxter International Inc - Denver, NC November 2016 to Present Managed team activities and established schedules for project deliverables. Developed Security Assessment Plan (SAP) prior to holding kickoff meeting with the System Owner; Conducted interviews with key client stakeholders to determine the security posture of the system. Developed and updated System Security Plan (SSP) and Security Assessment Report (SAR) Created plan of action and milestones (POA&M) and managed remediation Created and documented POA&M reports and corrective action plans Developed Business Impact Analysis, Contingency Plan, Continuous Monitoring Strategy, Security Assessment Plan, Risk Assessment Plan and Incident Response Plan. Continuously monitored the security controls, including analyzing and documenting changes to the information system. Performed vulnerability scans using Nessus, CIS-CAT, Acunetix and Microsoft Baseline Security Analyzer. Performed testing and implementing network disaster recovery plans. Performed risk assessments and testing of data processing systems. Great familiarity with firewalls, data encryption and other security measures. Recommend security enhancements and purchases. Trained staff on network and information security procedures. Reviewed of security document updates by ISSO. Ensured software is patched and able to protect from threats. Made recommendations for mitigating

identified risks. Monitored live systems to discover real-time threats. IT Security Analyst Tempus Resorts International Orlando, FL May 2014 to November 2016 Developed Security Assessment Plan (SAP) prior to holding kickoff meeting with the System Owner; in conjunction with the Project lead interviews with key client stakeholders to determine the security posture of the system. Developed and updated System Security Plan (SSP) and Security Assessment Report (SAR) in conjunction with the Project lead Created plan of action and milestones (POA&M) and managed remediation Created and documented POA&M reports and corrective action plans Developed Business Impact Analysis, Contingency Plan, Continuous Monitoring Strategy, Security Assessment in conjunction with the Project lead Performed vulnerability scans using Nessus, CIS-CAT, and Microsoft Baseline Security Analyzer. Education Associate degree in computer science in computer science University of Bamenda Bachelor's degree in Modern Letters in Languages University of Bamenda Additional Information CAP Cert in progress Risk Management Framework Training Introduction to Windows System Admin Introduction to Linux System Admin TECHNICAL EXPERIENCE / SKILLS CSAM Exacta Protocols and Services - [DHCP DNS TCP/IP SSH FTP SFTP SCP Ping SMTP POP3] Excellent problem-solving skills - able to identify, analyze and propose solutions to technical and business issues Enterprise security knowledge Intrusion analysis and Knowledge of IDS systems Computer and incident investigation and response experience Experience with network packet analysis using Wireshark Log analysis and experience reviewing security Events using Splunk Experience in investigating various types of cyber attacks Excellent troubleshooting skills especially working with windows suite of application and OS Adept with Network protocol and service Exposure to various vulnerability management tools such as Nmap, Retina, and Nessus Evaluate emerging technologies for suitability and competitive advantage

Name: Debbie Dawson

Email: nancy30@example.net

Phone: 446-444-3428x271