Security Manager IT Security Manager IT Security Manager IT - Coal fire Labs New York, NY Enterprise Information Security Technologies experience with focus on Information Security, Application Security, IT Governance, IT Risk Management, Compliance and IT Audits with specialization in Security analysis, design, development and testing of applications in n-tier architecture and Systems Security Certified ISO 31000 Lead Risk Manager Certified ISO 27001 Lead Auditor SANS GIAC certified in Information Security Policy (GFSP) Experience with IT Compliance and Audit Standards of ISO, SOC and SSAE Knowledge of 21 CFR Part 11, Annex 11 Regulations and Good Manufacturing Practice (GMP) Governance and Compliance experience with ISO 31000, COBIT, ISO 27001, PA DSS, PII and PHI Strong understanding of information technology controls and security experience in a widely used financial application environments like (SAP, Oracle, JD Edwards, PeopleSoft, etc.) Provided Project Management by defining ITIL Project goals, managing resources, maintaining project time lines and leading multi-discipline teams while fostering input from various levels Experience in Audit in ISO 27001-2 standards in domains of Security Policy, Incident Management, Cloud, Business Continuity/Disaster Recovery, Access Control, Asset Management and others Managed and lead Business Continuity (BCP) and Disaster Recovery process (DRP) Experience with Cloud technologies and implementation of SAAS based security controls. Experience managing Projects based on Agile Methodologies including ITIL, COBIT and CMMI Experience leading and managing IT Risk, Governance, Security and Audit frameworks (COBIT, COSO, ISO 27001/2/5, NIST 800-53, SSAE 18, SSAE 16) Experience in developing a compliance schedule tailored for SSAE 16/SOC and ISO 2700x Audits Experience and strong knowledge of Internal Controls over Financial reporting including SOX 404, SOC 1 Audit reports, COSO, US GAAP, ITGC, PCOAB and IIA Standards Managed and lead Regulatory & legal security standards such as PCI DSS, Sarbanes-Oxley, HIPAA Managed and provided regulatory expertise and solutions on complex risk and compliance issues based upon understanding of business unit's activities and products. Managed and lead projects involving Security best practice frameworks - COBIT, NIST 800.x, ITIL, ISO 27001, ISO 27002, ISO 27005, HITRUST, PCI, SOX, FED RAMP and FFIEC Managed Regulatory Compliance implementation

with OWASP, FISMA, HIPAA, PCI- DSS, GLBA, SOX, COBIT, COSO, FFIEC, NIST, ISO and GDPR Several years of technical experience in Information Security, in an environment certified and compliant with globally recognized Security Frameworks and maintained Compliance with GDPR, PCI, COBIT, SOX, NIST, ISO 27001 and ISO 27018 Controls Experience with Web App Security tools with an understanding of Application security Experience with Cyber Security compliance and regulations and knowledge of NY DFS Cyber Security rules and regulations. Knowledge and experience with NERC CIP and SSAE-18 Compliance, ERP Systems Experience with computer security procedures and protocols and experience with Security Information Event Management tools (SIEM), Intrusion Detection & Prevention Systems (IDS/IPS), Firewalls & Log Analysis, Network Behavior Analysis tools, Antivirus, and Network Packet Analyzers and malware analysis. Monitored Security State and managed continuous monitoring Experience with Web application development using Java, .NET(C#) Implemented Security Controls, Common Security standards, Practices and Risk frameworks - FAIR, NIST, OCTAVE, STRIDE, ISO 27005 and ISACA Experience with Payment Card Industry (PCI DSS, PA-DSS, P2PE) Knowledge and understanding of Cryptography -PKI, PGP, SSL, SSH Technical experience with Systems networking, databases, Web development, and user support. Involving in the design phase of any new IT software development and Security projects. Involved in building, supporting IT Security systems and associated subsystems within GE setting. Involved in Risk Assessment and GAP Analysis performing GAP analysis w.r.t. security and Compliance of regulatory standards and reported Risk factors. Experience with cloud technologies and implementation of SaaS based security controls. Knowledge of Information Security Controls and Standards, particularly ISO 27001/27002 and NIST 800-53, Rules and Regulations related to Information Security and Data Confidentiality with Application, Database, Network Security Principles for Risk Identification and analysis. Exposure to Threat Modeling using STRIDE, Penetration, Security testing, Code Security reviews Application Security Planning and Security Architecture Work Experience Security Manager IT Coal fire Labs - Atlanta, GA August 2017 to Present Coal fire Labs Responsibilities: Responsible for performing Security Risk Assessments, managing Vulnerability Management

Program and implementing Controls with Regulatory requirements of HIPAA, PCI DSS, GDPR Provide Project Management and strategy in all aspects of IT, Business risks and Audit engagements Managed IT Compliance and Security of Audits, Compliance checks and assisted external assessment processes for Auditors, Payment Compliance Industry (PCI), Personally Identifiable Information (PII), General Data Protection Regulation (GDPR), HIPAA and SOX Compliance Responsible for ensuring Security and Compliance with PCI DSS, ISO 27001, HIPAA, HITRUST, SOC II as well as company security requirements Worked with Top Payment Application Clients in the industry for PCI and HIPAA, HITRUST CSF, and Compliance to meet Information Security requirements and Security Maintenance Managed, developed and executed Annual IT Audit Plans as well as Testing IT Processes Managed and conducted IT Audit on overall Information Security aspects for each client covering User & Access Management, Database Access & Network, Data Storage, Internet, Intranet, Audit trails & Data Privacy Protection management Experience with Internal Controls, Risk Assessments, Business Process and Internal IT Control testing and Operational Auditing Involved in performing Audits and Internal testing of Controls annually around ISO 27001, FISMA audits and other IT Risk areas as needed Participate in Internal and External Audits and coordinate into Security Services activities Experience in performing Auditing and other testing of Security Controls, developing Audit Plans and Procedures and reporting the results of such audits Manage GDPR Compliance overview, Road mapping, Program development and Implementation Manage and lead GDPR Program Management, Regulatory Compliance mapping and monitoring Managed and delivered IT Risk Assessments and Audits on various projects involving IT Governance and Strategy, DRP, BCP Change Management and Cyber Security areas Experience in Payment Card industry, Credit card transactions and Audit of Payment Application logs and ensure PAN is rendered unreadable Managed Projects with Data Governance and Data Privacy, Created Plan of Action and Milestones (POA&M) Managed and Lead Business Continuity and Disaster Recovery Program including Business redemption, System Recovery and restoration and provided overall IT Support for Internal Clients Managed and lead development, implementation of relevant Metrics to measure the

efficiency and effectiveness of ISMS, Governance, Risk Management and Compliance programs across Coal fire Experience working with Risk, Security and Audit frameworks (COBIT, COSO, ISO 27001/2, ISO 27005, NIST 800-53, SSAE 16) and ISO 27018 controls Experience in Governance and Compliance for PCI PA-DSS, FISMA, PII and GDPR Assisted in the analysis of PCI Assessment findings, owner identification, remediation planning Experience in Information Security Policy creation and acceptance Experience in meeting PCI, PII and PHI requirements Involved in maintaining Data Privacy for GDPR, HIPAA, FDR and lead SOC 2 and HITRUST Audits Implemented Data Protection Governance Practices, Privacy Impact and Gap Assessments Involved in Cybersecurity Controls Assessment delivered using best practice frameworks including NIST CSF, COBIT 5, CIS and other frameworks Implemented SaaS based Cloud security Controls Involved in working with Information Security Analysts and application & service owners with PCI-DSS compliance tasks such evidence preparation, gathering and submission to the PCI-DSS assessor for annual compliance Collect and evaluate evidence and prepare reports and documentation in an appropriate format. Involved in working with Payment Card Industry (PCI DSS, PA-DSS) and P2PE relevant projects. Assisted in filling out ROVs and ROCs for numerous Clients including POS applications Involved in creating No Impact Change Reports and Low Impact Change Reports. Evaluated Customer Network and Data Flow Diagrams Validated technical controls of PSS Data Standard Created White Papers through Client Documentation and review Involved in implementation of System Security Software and other Forensic tools Evaluated Payment Applications using Wire Shark Forensic Tools. Exposure to PKI and Asymmetric and Symmetric encryption Utilized Control Routines and Risk Management Policies to identify and analyze risks Environment: ITIL, PCI DSS, P2PE, HIPAA, GDPR, FTK, GRC Archer, NIST RMF, OCTAVE, STRIDE, FED RAMP, Wire Shark, PKI, NIST CSF, Oracle, UNIX, Java script, SQL, HTML, ISO 27005, Cyber security, NERC CIP, SSAE-18 SOC 1, ISO 27018 VP Senior IS Tech Analyst Citibank - Fort Lauderdale, FL April 2015 to July 2017 Technology, Security and Operations Responsibilities Managed Audit in meeting GLBA Compliance requirements and FFIEC Compliance Managed Bank IT Audit implementing best practices and meeting Regulatory

Compliance needs and provided Audit reports to improve Bank IT Security Program Managed Bank IT Risk assessments IT Compliance, Audits, GLBA Audit and Internet Banking Audit, Managed Bank Disaster Recovery Plan and Bank's Business Continuity Program Manage Risk Assessments internally and externally and support a large-scale global enterprise and set direction as a leader Managed BC/DR program including BIA Analysis, DR Plan documentation, BC and DR exercises, emergency management communications across Banking divisions during Cyber events/outages Managed and involved in all aspects of Risk Management including implementation and monitoring Risk Management process in the organization. Managed Audit activities for a functional entity at Regional level including a portion of Annual Audit Plan along with managing Annual Audit Work Plan Managed IT Audits, Information Technology Risks and Controls, Information Security & Governance Hands on experience overseeing and implementing the Global SOX, ISO 27001 Control Frameworks across Citi Global IT environment. Managed and developed Information Security Standards, Procedures, Policies and guidelines along with Application architecture and threat modeling Involved in defining Bank's Information Security Program, Policy and Standards Coordinated with Corporate and Investment Banking (CIB) team members, IT Risk Managers, local management and Global CIB when needed to provide reasonable assurance that Security Program and IT Governance processes and Controls are properly implemented and Corrective actions are taken where needed. Involved in ensuring Risk Management in coordination with different Stake holders of Risk, IT Risk Management Group, OPC, Compliance, Regulatory affairs and Supervisory relations Involved in implementing Safeguarding Standards and provided implementation in relevance with NIST Cyber Security Framework (CSF) incorporating it into Risk Management. Evaluated Applications using Static Coding analysis tools - Vera code, IBM AppScan Tools and provide Application Vulnerability Assessment services (Dynamic and Static) to all Citi businesses and technology teams globally Involved in evaluating current risks and provide recommendations for Risk Tolerance and Mitigation. Collaborate with Stakeholders to document and implement necessary Policies and Procedures to comply with ISO 27001 Standards and to obtain Certification. Implemented Security Controls across technology

stack to meet Security and Compliance requirements for IaaS, PaaS, SaaS Participate with leaders in definition and implementation of Information Security Policies, Strategies Involved in creation and maintenance of new Policies and Procedures enhancing the existing Policies, Procedures and IT Risk requirements as needed. Source Code Reviews and OWASP Secure Coding Practices Experience in Security Policy development, writing, security education, Application Vulnerability assessments, Risk Analysis and network penetration testing Assisted in driving day to day activities and execution of PCI Program across Citibank Worked with Policy and Standards team to integrate PCI Compliance aspect into Citi's current Policy and Risk Management Process. Environment: ITIL, ISO 31000, ITIL, SOX, COBIT, IBM AppScan, Vera code, Oracle, UNIX, Java, SQL, HTML, JavaScript, PCI Compliance, ISO 27001, GRC Archer, FAIR, STRIDE, OCTAVE, NIST RM, NIST CSF, ISO 27005 Applications Security Analyst General Electric (GE) Capital - New Orleans, LA August 2013 to March 2015 IT Security and Operations Responsibilities Responsible for Internal Controls and Risks of GE Capital Bank Technology network Involved in Planning and execution of Internal Audit procedures and creation of Internal Audit reports. Experience in Audit Log reviews and SOC Operations support Managed Security Policies, Procedures and responded to security reviews Reviewed system Audit logs in accordance with the SSP Managed and involved in performing manual Security architecture risk analysis, thread model reviews of applications and assess their design against known or emerging threats Managed, driven remediation efforts related to Information Security, Remediation for Incidents, Vulnerability Scans, Pen tests, Internal and external Audits and Critical Practice assessments. Lead Vulnerability remediation efforts for identified issues on Systems, devices and Network devices with System owners Assisted in managing an outsource relationship for 3rd party application development Lead trouble shooting technical issues and identified modifications needed in existing applications to meet the changing user requirements and managed risk with reference to NIST Cyber Security Framework (CSF) and mitigate Cyber Security events Responsible for analysis, design and implementation of System Security Software upgrades Enterprise level Information Security Architecture , coordinated Information Security procedures and controls, application testing

and security incident response Analyzed and tested new and existing procedures, information systems and utility programs for security vulnerabilities and recommended remediation procedures. Coordinated application development with Code Scanning with HP Fortify for multiple projects. Assisted in Source Code Analysis, Remediation and troubleshooting of application security issues. Analyzed data contained in the corporate database and identified data integrity issues with existing systems and proposed system solutions. Assisted System analysis and design of security requirements for GE Security & Operations division Managed and lead Security Development Lifecycle (SDL), system development life cycle and Programming with Internet facing applications using Java and C# Analyzed Action plans for application vulnerabilities and provided remediation plans Involved in Firewall Policy evaluation, review and design Recommended alternatives for application security and issue resolutions Deliver reporting to Security Leadership on Remediation efforts Assisted various divisions of GE in the implementation of Software Security and Systems software Involved in identifying Application Vulnerabilities and implementing Security Practices for Cloud and Big Data Computing Environments Involved in educating Security awareness with end users Retrieved data to prepare documents, and produced a variety of reports from databases Creates and generated documentation concerning security procedures and maintenance of Reports Assisted in maintaining a System Security Plan (SSP) and Security Testing Assisted in updating OS software and antivirus definitions in accordance with the SSP requirements Participated in weekly meetings with the IT Security and Network team to discuss progress and issues to be resolved, and report progress on a weekly basis to the Team Manager. Deliver reporting to Security Team leadership on remediation efforts Experience in running Vulnerability Management tools and utilize manual techniques to identify and validate closure of security issues. Environment: ITIL, NIST RMF, STRIDE, UNIX, HP Fortify, Vera code, Qualys, Java, .Net, C#, Oracle, Java script, SQL, HTML, Information Security Contract Consultant Developer Softcon USA Inc - Maywood, IL February 2010 to July 2013 Project: Online Marketing Responsibilities Programmed PHP back end web services for Remote Flash application. Involved in the development of MySQL procedures and maintaining reports in SSRS Involved in evaluated the company's PHP based

website code and accompanying MySQL database Environment: Crystal Reports XI / 2008 / 2011, SSRS, PHP 5.0, Java, MySQL 5.0, Adobe FLEX 3.0, Action script 3.0, MXML, Flash, HTML/DHTML, Java script, XML, CSS, Subversion, Linux Client: Riverside Publishing, Rolling Meadows, IL Consultant: Developer / Consultant Project: Product Service Management Responsibilities Implemented Product configuration management using Java Programming using Adobe Lifecycle Data Services ES for automatic paging of large data sets, real-time data synchronization Implemented enhancements in Enterprise level Java Application and handled Environment: Crystal Reports XI, Java, Adobe Flex 3.0, ActionScript 3.0, MXML, Spring Framework 2.5, Hibernate 3.2, Flash, Oracle 10g, HTML/DHTML, XML, CSS, Flex Unit, JUnit, Java script Consultant Ajilon Consulting Inc - St. Louis, MO May 2006 to December 2009 Senior Developer/ Consultant Project: Smart Trade Responsibilities Designed and developed all parts of the Web application-including configuring Spring and Hibernate Involved in driving the technical design to support Business application using Java/J2EE technologies Followed agile software development with Struts methodology. Implemented the persistence layer using Hibernate ORM. Used JIRA to assign, track, report and audit the issues in the application Environment: Core Java, Servlets, JSP, J2EE, Spring 2.5, Struts, HTML, Web services (using AXIS), Eclipse 3.1, UML, Maven, WebLogic 9.1, Oracle 10g, JUnit, Log4j, Hibernate, SQL Scottrade Saint Louis, MO Consultant: Developer / Analyst Project: Collateral Advisor Responsibilities Implemented collateral management using Java and MVC Created top N, parameterized and drill down Crystal Reports for BI needs with Oracle tables. Involved in Creation of User interfaces and Action script development with Adobe Flex Environment: Crystal Reports XI, Adobe Flex 2.0, Adobe Flash, ActionScript, XML, XSLT, HTML, JUnit, Client: Health Care Service Corporation (BCBS), Chicago, IL Consultant: Java Consultant / Developer Project: Claim Optimization and Change Management System Responsibilities Involved in Programming using Java and JDBC Implementing enhancements in Enterprise level Java Application. Developed and Integrated Crystal Reports with enterprise and created Custom components to automate the notification process in case of rejection/completion using Swing Environment: Crystal Reports XI, IBM WebSphere 6.0, MVC,

Java, JSF, Servlets, Applets, JDBC, PL/SQL, Oracle 10g, JSP, JUnit, XML, XSLT, UNIX Client: Emerson, Saint Louis, MO Consultant/ .Net Developer Project: Winning Inventory for Sales Escalation Responsibilities Involved in Programming using C#, ADO.NET and XML Involved in creation of database objects (Database Tables, Indexes and Views) with Oracle 9i Created parameterized Sub Reports with various chart types for using Crystal Reports &SSRS Environment: SSRS, C#, ASP.NET, ADO.NET, CLR, XML, Visual Studio 2003 Environment, PL/SQL, RUP, Oracle PL/SQL, Crystal Reports Java Consultant McNally Systems Inc - Lansing, MI January 2005 to April 2006 Project: E-Mortgage Prequalification Responsibilities Designed and developed functionalities for the fixed assets management module in MVC Pattern Involved in writing SQL queries to access data from the database. Developed and maintained stored procedures (PL/SQL), SQL scripting Environment: Java, Servlets, JSP1.2, EJB 2.0, HTML, Java script, XML, Struts, Oracle 9i, PL/SQL, Windows 2000, JUnit, UNIX Client: State Department of Michigan- Lansing, MI Department of Community Health (DCH) Project: Children's Special Health Care System (CSHCS) Consultant: Java Consultant/Contractor Responsibilities Programming Java, Servlets, JDBC, Design patterns Involved in writing Procedures in PL/SQL and Triggers Involved in Application Design and Development and generating Oracle Reports 2.5 Environment: IBM Web sphere, JAVA, Beans, JDBC, ORACLE 9i, EJB, JSP, SQL, PL/SQL, Oracle Reports 2.5, UNIX, JavaScript, JUnit Education Bachelor's Skills HTML (10+ years), JAVA (10+ years), ORACLE (10+ years), SQL (10+ years), UNIX (10+ years) Additional Information TECHNICAL SKILLS Project/Program/Portfolio Management ITIL, COBIT, ISO, Agile, PMI Compliance & Audit GDPR, Fed Ramp, FFIEC, SOX, NIST, PCI, HIPAA, FISMA PCI COSO, PA DSS, PCI DSS, P2PE, SSAE 18 SOC 1, SSAE 16 IT Security Tools FTK, Wire Shark, Nessus, Encase Vulnerability scan tools Qualys, HP Fortify, IBM AppScan, Vera Code Business Intelligence SSAS, SSIS, SSRS, BOE Crystal Reports XI /2008 / 2011 Data Bases & Data Analytics SQL, SQL Server 2008/2012, Oracle, PL/SQL Languages & Web JAVA, C#, Ruby, PHP, C, Pascal, COBOL, HTML, XML, TCP/IP Reporting Tools , Oracle Reports, Crystal Reports, SSRS Operating Systems UNIX, Linux, Sun Solaris, Windows XP/98/NT/2000

Name: Diane Carter

Email: timbutler@example.com

Phone: (937)217-1340x260