|  |  |
| --- | --- |
| 2126 Faulk Drive  Tallahassee, Florida 32303 | Phone: 850-445-8811 (cell) – Primary  Email: [ed\_cissp@yahoo.com](mailto:ed_cissp@yahoo.com) |

Charles Edward Wilson (C|CISO, CISM, HISP, FITSP-A, FITSP-M, MTS, ISSM, ITIL)

|  |  |
| --- | --- |
| Summary of Qualifications    Certifications  2016/2017 Certifications  Education  Professional Experience | A recognized expert in Information Security Management & Privacy Services who is focused on delivering Public and Private Sector Information Security & Privacy Services. Has a diverse, 37-year background in IT Security and Compliance including 20 years as a Cryptologist in the US Navy, six (6) years as a Threat Analyst and Security Compliance Advisor for the National Security Agency (NSA), and 20 years in Healthcare Data Management.  Have designed and overseen the secure implementation of IT risk organizations, emerging technologies (wireless and cloud computing) and world leading e-commerce solutions. Designed control frameworks allowing companies to be fully FISMA, HITRUST, PCI compliant as well as ISO 27001 compliant. Have high-caliber presentation and communication skills and a highly sought after speaker on Cyber Security, Risk Management, INFOSEC, Incident Response, HIPAA Privacy/Security, Business Continuity and Disaster Recovery (BCP/DRP), and Regulatory Compliance regarding HIPAA, FISMA, PCI DSS, SOX, and GLBA.  Demonstrates working knowledge and understanding system security, controls or information security management environment in the following Healthcare and Information Security domains:     * + Information Program Management   + Healthcare Information Technology Security and Privacy   + Regulatory Compliance (HIPAA/HITECH, FISMA/NIST, COBIT, HITRUST, ISO 27001, PCI DSS, SOX, and ITIL)   + Policy Development & Management   + Security Function Design   + Corporate and IT Governance   + NIST Risk Assessment/Management   + DIACAP   + NIST Risk Management Framework (RMF)   + IT General Controls Auditing   + Cloud Security and Auditing   + Strategic Security Planning   + Security Architecture and Strategy   + Threat & Vulnerability Management   + Identity & Access Management   + Network Security & Architecture   + Cybersecurity   + Incident Response   + Attack & Penetration Testing   + Business Continuity Planning/Disaster Recovery Planning (DRP)   + Security Awareness, Training, & Education   + Data Loss Prevention (DLP)   + Health Information Exchange and Patient Health Record Systems   + Auditing & Log Management   + Mobile Device Security & Strategy   + Business Associate and Third-Party Risk Management   + Large Complex Security Program Execution/Implementation   + Security Infrastructure      * [C|CISO](http://cert.eccouncil.org/certified-chief-information-security-officer.html) Certified Chief Information Security Officer (C|CISO) (ECC88513168442) (29Mar2013) * [CISM](http://www.isaca.org/About-ISACA/Press-room/Pages/CISM-Fact-Sheet.aspx) Certified Information Security Manager (CISM) (Member No. 0301047) (4Sep2003) * [HISP](https://www.hispi.org/about.php) Holistic Information Security Practitioner (HISP) (Member No. 100015) (24Mar2006) * [FITSP-M](http://www.fitsi.org/Overview/index.htm) Federal IT Security Professional-Manager (FITSP-M) (Member ID. 400) (18Jan2011) * [FITSP-A](http://www.fitsi.org/Overview/index.htm) Federal IT Security Professional-Auditor (FITSP-A) (Member ID. 400) (18Jan2011) * [ITIL](http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library) Foundation Certification versions 2 and 3 * [IT-2779](http://usmilitary.about.com/od/navynecs/p/IT2779.htm) Information System Security Manager (ISSM) * [IT-2735](http://usmilitary.about.com/od/navynecs/p/IT2735.htm) Information Systems Administrator (ISA) * [IT-2780](http://usmilitary.about.com/od/navynecs/p/IT2780.htm) Network Security Vulnerability Technician (NSVT) * [CTT-9170](http://usmilitary.about.com/od/navynecs/p/CTT9170.htm) CLASSIC WIZARD Basic Operator * [CT-9168](http://usmilitary.about.com/od/navynecs/p/CT9168.htm) Advance Non-communications Collection and Analysis Technician * Cryptologic Technical Technician First Class Petty Officer (CTT1) * Department of Defense Technical Training Instructor * Department of Defense Master Training Specialist (MTS) * Microsoft Certified Professional (MCP) * Technical Writer and Curriculum Developer * Prosci Change Management * Currently preparing for the following certifications:   + (ISACA) Cybersecurity Fundamentals Certificate (CSX)   + (ISC)² Certified Information Systems Security Professional (CISSP)   + EC-Council - Certified Ethical Hacker (C|CEH)   + EC-Council - Certified Incident Handler (C|CIH) * **Currently studying towards a BA in Information Systems Management (IFSM) from University of Maryland – 96 credits completed to date** * Task Based Curriculum Development and Technical Writing * Check Point FireWall-1 4.0 Certified Security Administrator * Check Point FireWall-1 4.0 Certified Security Engineer * ADPSO Concepts and Risk Management Auditing * Information Systems Security Management (A-531-0009) three weeks * Information Systems Administrator (A-531-0046) eight weeks * Network Security & Vulnerability Technician (A-531-0022) eight weeks * Department of Defense (DoD) Technical Training Instructor 12 weeks * Configuration Management (D-555-0048) three weeks * Federal Information System Audit Controls – NIST SP800-53 (1 week) * Fundamentals of an Internal IT Auditor (3 days) * Project Management 1 & II * Software Quality Assurance and Testing * Identifying and Confirming User Requirements * Effective Skills for Technical Managers * Influence Skills   Oct 2011 – Present Capital Health Plan Tallahassee, Florida  ***Fulltime:*** **Information Security Manager (ISM)**   * Responsible for meeting regulatory compliance regarding Cybersecurity, HIPAA, FISMA, PCI DSS, Fraud, and Financial Audits regarding general security controls. Report to the Chief Information Officer. * Responsible for oversight of all ongoing activities related to the development, implementation, maintenance, and annual reviews of 135 enterprise Compliance Policies, Procedures, and Standards to safeguard protected data held by the organization in accordance with federal and state laws. * Maintain the Cybersecurity Management and Information Security Risk Management Programs in accordance with National Institute of Standards and Technology (NIST) Standards and Guidelines and ISO 27000 Series Standards to data classification, Security control implementation, regular verification of security control performance, breach preparedness planning and testing, risk acceptance and risk transfer and Data Loss Prevention (DLP) initiatives are successfully working and information data and assets are protected across the organization. * Chair the weekly Security Steering Committee meeting with the CIO, Directors, Managers, and Executive Assistant to report the status of the Information Security Risk Management Program and Plan of Action & Milestones (POA&M) remediation efforts. * Provide technological leadership and guidance to Senior Management in delivering security solutions to meet or exceed organizational goals and business objectives. * Established and maintain three-year Strategic Security Plan to communicate Senior Management’s Policies and guide the development of standards, procedures, guidelines to include strategic planning initiatives. * Have oversight responsibilities of PCI-DSS regulatory compliance. Strengthened PCI environment with new governance, controls, documentation management system and information security training program across 16 Departments. * Responsible for overall maintenance of the Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) and Hurricane Plan. Work with Senior Management and 16 Department Supervisors to document, train, test, and update BCP/DRP and Hurricane Plan annually. * Assist the IT Director and Director of Programming and E-Commerce with security design and architecture decisions for all legacy systems and also during the SDLC for new systems and applications that will process, transmit, or store sensitive information as defined within the Data Classification Policy and Data Classification Matrix using the NIST SDLC methodology and/or Agile software development methods. * Developed and implemented policies and standards governing intrusion detection and intrusion detection configuration and deployment. Audit intrusion detection configuration to ensure that they are configured in accordance with the guidelines provided by policy. * Member of the Information Security Leadership Team and Change Advisory Board (CAB) that meets weekly to ensure changes are documented, tested, approved, and made in a controlled fashion to preserve the confidentiality, integrity and availability of the applicable system. * Submit quarterly Information Security Program Reports that address the current state of the Risk Management Program and POA&M remediation status to the Compliance Committee Board and Audit Committee Board. * Established and maintain an Incident Response Plan to ensure an effective and timely response to information security incidents. * As Incident Response Leader for all investigations, receive reports of any internal/external security breaches, malicious activity, and take appropriate action to minimize harm, investigate breaches, document accordingly, and identify corrective actions. * Continuously monitor the Data Loss Prevention initiative. Work closely with Information Technology Systems Support (ITSS) network technicians to monitor systems development and current operations (e.g., McAfee Change Control, McAfee Email Gateway) for HIPAA Privacy and Security compliance. * Enhanced the Risk Management Program by implementing the six-steps identified in the Risk Management Framework (RMF). This structured process integrated information security and risk management activities into legacy systems and new systems that will go through the SDLC process. * Enhanced the Risk Management Program by implementing the NIST Cybersecurity Framework to routinely Identify, Protect, Detect, Respond, Recover from risks. * Coordinate the annual network third-party enterprise vulnerability scan, penetration test, wireless assessment, and develops appropriate POA&M remediation for identified vulnerabilities. * Conduct annual HIPAA Privacy/Security and Meaningful Use Risk Assessment. * Developed and conduct a Security Checklist for all new eCommerce and/or Software-as-a-Service (SaaS) Providers as part of the organization’s Breach Notification Procedures. * Developed third-party monitoring procedures to conduct annual Physical Security Walkthroughs and gather all documentation (e.g., SSAE-16, Risk Assessments, and/or Audits) to ensure third-party regulatory compliance (e.g., HIPAA, PCI) is met. * Responsible for collecting and reviewing all third-party SSAE-16’s to ensure regulatory compliance is met. * Engage and directs third-party consultants as appropriate on all Financial and IT Audits. * Developed and maintain the Mobile Device Management strategy for the organization.   Mar 2016 – Jun 2016 Security Exchange Tallahassee, Florida  ***Fulltime:*** **Information Security Consultant / Project Manager**   * Provided Minimum Acceptable Risk Standards for Exchanges (MARS-E) compliance services to a State sponsored health insurance exchange to meet the Patient Protection and Affordable Care Act (ACA) of 2010. Developed and documented FIPS-199 System Categorizations for five (5) systems, detailed System Security Plan (SSP), NIST SP800-53 Baseline Security Controls, Three-year Continuous Monitoring Plan, and a Plan of Action and Milestone (POA&M) management and remediation plan. * Developed documentation for a Healthcare organization to implement the National Institute of Standards and Technology (NIST) Cybersecurity Standards. This allowed the organization to better protect patient data and prevent costly and damaging security breaches. * Developed a detailed Incident Response Plan in accordance with NIST SP800-61 Computer Security Incident Handling Guide for an organization that boasted their Incident Response Program as a key pillar of their security defenses.   Dec 2007 – Oct 2011 North Highland Tallahassee, Florida  ***Fulltime:*** **Information Security Manager / Project Manager**   * Trusted Information Security advisor to 26 state agencies on Regulatory Compliance for HIPAA, FISMA, PCI, SOX, COSO, GLBA, ISO 27001, HITRUST, COBIT, and ITIL. * Assisted in creating Project Management Office (PMO) to conduct risk assessments for 36 State Agencies. * Incident Response Manager charged with investigating an information breach at a National bank. As Manager of a team of four (4), coordinated all interviews, worked closely with law enforcement, and assisted with creating final incident report. * Project Manager of diverse teams of four (4) to nine (9) consultants to perform NIST based and ISO 27001 Risk Assessments for 24 State agencies. * Developed Low, Moderate, and High level System Security Plan (SSP) templates and used the templates to develop 23 Low, 55 Moderate, and 7 High level-impact SSP’s in accordance with the NIST SP800-18 Guide for Developing Security Plans for Federal Information Systems. Categorized all 85 systems in accordance with FIPS-199 Standards for Security Categorization of Federal Information and Information Systems.   Apr 2007 – Dec 2007 Intellect Technical Solutions Lakeland, Florida  ***Contract:*** **Information Security Consultant**   * Provided strategic oversight, responsibility, coordination of information security protection and security compliance efforts. * Developed 8 of 13 chapters in the new Information Security Policy manual which establishes Publix information security policies required for identifying information resources and supported business processes and appropriately protecting those information resources. * Developed the corporate Risk Management methodology and Audit Guidelines using the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30: Risk Management Guide for Information Technology Systems. * Developed the PCI DSS standard approach for the internal organization drafting a complete set of security policies and standards that cover each key security control area. * Developed the Disaster Recovery Plan Emergency Access Procedures for the Windows, UNIX, and Database environments.   Jul 2006 – Feb 2007 Craig-is Ltd. Jacksonville, Florida  ***Full-time:* Chief Information Security Officer (CISO) – Compliance Officer**   * Manager of eight (8) direct reports. Developed an organizational Information Security Policy Manual in compliance with ISO 17799:2005’s eleven domain requirements in support of the Information Security Management System (ISMS). Assumed overall responsibility for the organization’s data security and privacy policies, architecture, and procedures recommending security solutions including financial justifications and operational support options. Worked with the CIO to create, document, implement, and oversee policies, procedures, and practices that ensure the availability, integrity, and privacy of information assets. Provided appropriate access to and protecting the confidentiality and integrity of customer, employee, and business information in compliance with company policies and standards. * Developed the SAS 70 Type II audit standard approach for the organization. * Conducted internal Type II SAS 70 audit in preparation for third-party SAS 70 audit. Worked with third-party auditor in evidence gathering for testing and developed all remediation steps. * Prepared organization for ISO 27001 certification and accreditation. * Prepared and presented detailed audit findings to Senior Management; analyzing compiled data making recommendations to mitigate risks, improve processes and controls. * Chaired the Steering Committee and Information Technology Steering Committee leading efforts in the development and the delivery of the company’s security roadmap.   Jan 2006 – Jul 2006 Integrated Computer Solutions Inc. Tallahassee, Florida  ***Full-time:* Senior Security Consultant Project Manager**   * Project Manager of seven (7) consultants responsible for conducting six (6) PCI DSS assessments and drafted remediation plans to ensure that the set of twelve compliance requirements were met through implementation of standards for configurations, best practices, change management procedures, and validation processes. * Developed server hardening and firewall rule guidelines to ensure confidentiality, integrity, and availability which resulted in a substantial reduction in vulnerability exposure. * Developed Information Security Awareness and Training Programs for 12 State agencies. * Managed a diverse team of 12 consultants, vendors, and employees in the build-out of a new Security Operations Center (SOC) for a 1,500-person New York City-based law firm.   Mar 2005 – Dec 2005 DynTek Inc. Tallahassee, Florida  ***Full-time:* Information Systems Security Project Manager / IT Auditor**   * Executed audits of business controls, processes, and systems, in accordance with traditional internal auditing standards (ISO 17799, SAS 70, PCI DSS, COBIT, and COSO). * Implemented a PCI Data Security Program for eight (8) clients ensuring their security configuration will be “lock down” on those computer systems handling cardholder data. * Managed a team of four (4) to six (6) consultants to conduct Business Security Risk Assessment Audits utilizing ISO 17799/27001, NIST 800-53 Standards to identify gaps in the 24 State agencies. * Provided input into the state Computer Security Incident Response Team (CSIRT) establishing the roles, responsibilities, communications, and eDiscovery procedures for responding to computer security incidents, which may occur within the State of Florida’s government.   Nov 2004 – Mar 2005 Allstate/Ajilon Consulting Jacksonville, Florida  ***Contract (5 months):*** **Information Systems Security Project Manager / IT Auditor**   * Managed a SOX remediation project team of three (3) for Allstate IT Business Group. * Interfaced with external auditors and coordinated with internal teams to satisfy HIPAA and Sarbanes-Oxley concurrence requirements in synchronization with international best practices and regulatory requirements. Conducted internal SAS 70 Type II Audit and prepared organization for external SAS 70 Type II with third-party auditor.   Sep 2004 – Oct 2004 Landstar Systems, Inc./Ajilon Consulting Jacksonville, Florida  ***Contract (2 months):*** **Information Systems Security Project Manager / IT Auditor**   * Developed twenty-four (24) ISO17799/IS15408 security policies. * Developed nine (9) COBIT Audit Programs. * Recommended a comprehensive external and internal security architecture to protect the organizations network and components, which have been endorsed by management and incorporated into their remediation process. * Developed the System Development Lifecycle (SDLC) five phase approach that included a minimum set of tasks to incorporate security in the system development process.   Sep 2003 – Sep 2004 Tropical Shipping Inc. West Palm Beach, Florida  ***Contract (12 months):* Information Security Professional/Business Continuity Plan Project Manager**   * Responsible for the successful rollout of a Sarbanes-Oxley IT-wide Solutions Framework for standard IT audit compliance solution delivery across six VP portfolios. * Identified and implemented all internal security controls covering operational risk and IT-related risks in compliance with COSO and SOX sections 103 and 404 requirements for business continuity planning. * Developed eleven (11) IT Governance Policies. * Developed the organizations Business Continuity/Disaster Recovery Plans (BCP/DRP). Conducted BCP/DRP Training and Testing to ensure applicable employees were familiar with the Plans.   Jul 2004 – Sep 2004 Agency for Health Care Administration (ACHA)/CH2M Hill Tallahassee, FL  ***Contract (3 months):*** **Information Systems Security Project Manager / IT Auditor**   * Managed a team of eight (8) to conduct an audit of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by AHCA. * Audited the IT hardware, software, interconnected on-line systems, policies, procedures, and other physical, technical, and administrative safeguards of selected systems. * Developed a risk mitigation recommendation for eleven (11) system applications containing PII using the NIST SP 800-30 Risk Management Guide for Information Technology Systems to include the CMS Information Security Risk Assessment Methodology.   Apr 2003 - Jul 2003 iStaff Inc. Tallahassee, Florida  ***Contract (4 months):*** **HIPAA Privacy/Security Project Manager**   * As Project Manager worked directly with HIPAA Privacy Officer, Senior Management, and system experts by laying the foundation for HIPAA Security and Sarbanes-Oxley compliance analysis, documentation, strategies/recommendations and a documented plan for HIPAA and SOX 404 compliance, including a Business Continuity Plan (BCP).   Dec 2002 – Apr 2003 Anthem Insurance Inc. Indianapolis, Indiana  ***Contract (5 months):* HIPAA Privacy/Security Project Manager**   * Responsible for identifying and implementing Privacy and Security audit controls to mitigate risk ensuring the confidentiality, integrity, and availability of data privacy and the privacy of a patient’s Protected Health Information. Performed Privacy and Security Rule Risk Assessments. * Developed 18 security policies, standards, guidelines, and procedures across four regions.   Jul 2002 – Dec 2002 State of Georgia Department of Revenue Atlanta, Georgia  ***Contract (6 months):*** **Information Security Architect Consultant**   * As Information Security Architect and team member of six (6) under the guidance of the CIO, successfully created a state of the art Security Operations Center that monitored all DOR sensitive data to include the privacy of Georgia citizens private tax records. * Developed and Managed DOR incident response center. Ensured the implementation of overall security measures, in accordance with Internal Revenue Service (IRS) procedures. * Developed the IT Audit strategy, policies, and procedures which became the foundation of security for the State of Georgia and were implemented in 128 State of Georgia Agencies. The Audit policy was incorporated into the Internal Revenue Service 1075 Publication. |
| References | May 1999 – Aug 2001 Lucent Technologies Alameda, California  ***Full-time:* Chief Information Security Officer (CISO) – Security Operations Center (SOC)**   * As Manager of a Networked Security Engineer team of four (4) reporting to the Vice President successfully roll-out a Security Operations Center under budget saving the company 1.2 million dollars. * Managed the day-to-day client policy configuration, change control, firewall, revision control, and recommended and implemented actions for increased security protection in a 24/7 Network Operation Center (NOC). Serviced continuance strategies and plans during security attacks. Drafted high-level, tactical, and strategic recommendations for security requirements. Developed NOC Operations Manual that included 27 NOC policies and procedures.   Jun 1979 – Jun 1999 United States Navy (**Retired**)  **Cryptologic Technical Technician CTT1 (AW)**  **Chief Information Security Officer (CISO)**  **Instructor Information Security Management (ISSM)**   * As Information Security Subject Matter Expert developed the three-week (3) [IT-2779](http://usmilitary.about.com/od/navynecs/p/IT2779.htm) Information System Security Manager (ISSM) course consisting of 31 INFOSEC topics at the master level supporting the National Security Agency (NSA) and Information Security (INFOSEC) Program Operational requirements for the DoD. * Adjunct Lecturer on INFOSEC manners for the National Security Agency (NSA). Taught twenty-six (26) National Cryptologic School courses for the NSA to 432 students. * As Information Systems Security Manager acted as Security Certification Committee Steering Chair on SDLC development life cycle projects for five (5) Research and Development centers with over 750 applications of which 273 were sensitive or critical. * As Project Manager, managed all phases of system design technical specifications on nine (9) High and Moderate level-impact systems using NIST SP800-64 Security Considerations in the System Development Life Cycle.   References are available upon request. |