**Ketrica R. Green**

***300 N. Akard St.***

***Dallas, TX 75201***

***Cell: 254-702-2582 ketrica2002@yahoo.com***

**SUMMARY**

Over 14 years of progressive Information Assurance (IA), System Security and System Administration experience. Extensive experience with Information Technology (IT) operations through all phases of large-scale technology including security, risk analysis, policy development, computer forensics, network migration, and experience with Automated Tracking Systems. Including expertise in the following areas:

|  |  |
| --- | --- |
| * Information Assurance/Auditing | * PCI, HIPAA, NIST, E&Y, ISO 27001 and 27002 |
| * Configuration Management/C & A | * Organizational Development and Training |
| * Strategic Planning/Project Management | * Data Encryption/Vulnerability Assessment/SOC2 |
| * ERP Planning/Program Management | * Incident Response/Firewalls/MS Win Hardening |
| * IT Governance/Compliance/SOX * Financial Management/Budgeting experience for IT Department | * ITIL/COBIT/Six Sigma for IT Systems/Scripting * Risk Management/IS Management/Disaster Recovery * Network Security/Digital Evidence Handling i.e. PII/PHI |

**PROFESSIONAL EXPERIENCE**

**engility**, Irving, Texas  **SEP 2016 – Present**

**Chief Information Systems Officer (CISO)**

Supports Third Party Information Security Risk Reporting, Assessment, and Mitigation. Provide major input on from a security standpoint within the organization’s global security initiatives. Information Security Control Privacy Manager responsible for implementation and monitoring of security and privacy controls to ensure protection of system data for healthcare information systems.

* Provide support to the Enterprise Technical Management Support Services (ETMSS) Chief Information Security Officers as may be needed on developing security and privacy artifacts. Security Control Privacy Manager responsible for implementation and monitoring of security and privacy controls to ensure protection of system data.
* Performed oversight of the development, implementation, and evaluation of information system security program policy. Performs network penetration testing. Performed Third Party Accreditation and Assessments of PHI based Information Systems utilizing the Risk Management Framework.
* Develop processes and tools for annual due diligence requirements and risk-based dashboards for a centralized view of Client Third Party Suppliers Information Security posture. Supports Third Party Information Security Risk Reporting, Assessment, and Mitigation
* Performed enterprise security monitoring and reporting. Maintained security infrastructure & cyber-security operations to mitigate identified risks, to meet business objectives and to meet regulatory requirements. Supporting field team members in cyber-centric life cycle management services to clients after fielding of the system including patch validation & deployment, vulnerability management, log review, incident response, etc.

**Ketrica R Green Page Two**

**Keatrin TECHNOLOGY**, (Remote)  **SEP 2016 – Feb 2017**

**Sr. Cyber Security Architect**

Supports Third Party Information Security Risk Reporting, Assessment, and Mitigation. Managed and performed security engineering analysis, risk analysis, and vulnerability studies on systems and applications under development by the Department of Defense. Provide major input on from a security standpoint within the organization’s security initiatives.

* Performed enterprise security monitoring and reporting. Maintained security infrastructure & cyber-security operations to mitigate identified risks, to meet business objectives and to meet regulatory requirements. Supported/Implemented key security applications - Web Filtering (WebSense), Anti-Virus (MacAfee), Firewall (ForcePoint), DLP and Monitoring (Digital Guardian).
* Perform forensic activities as required during corporate investigations. Managed incident and Change Request service levels according organizational guidelines. Provided a strong understanding of Security Information and Event Management (SIEM) technologies such as MacAfee EPO
* Collaborates with systems administrators in implementing corrective actions required as result of vulnerabilities uncovered during system scans in coordination with Information Assurance Manager (IAM) and IA Program Manager Guidelines.
* Evaluated, configured, and recommended new, disruptive, innovative technologies AWS (cloud), Splunk (analytics) that require an integrated security architecture.
* Managed Splunk knowledge objects (Apps, Dashboards, Saved Searches, Scheduled Searches, Alerts,
* Interfaced with cross functional teams to create potential mitigation solutions for risk areas and track them to resolution. Created Plans of Actions and Milestones to continuously monitor non-mitigated findings.
* Assessed Third Party Supplier’s information security risk posture to ensure compliance with Federal regulations, guidelines, and industry best practices.
* Collaborates with systems administrators in implementing corrective actions required as result of vulnerabilities uncovered during system scans in coordination with Information Assurance Manager (IAM) and IA Program Manager Guidelines.
* Interfaced with cross functional teams to create potential mitigation solutions for risk areas and track them to resolution. Created Plans of Actions and Milestones to continuously monitor non-mitigated findings.
* Assessed Third Party Supplier’s information security risk posture to ensure compliance with Federal regulations, guidelines, and industry best practices.

**Ketrica R Green Page Three**

**CITI**, Irving, Texas  **AUG 2014–JUN 2016**

**Sr. Cyber Security Engineer**

Develop processes and tools for annual due diligence requirements and risk-based dashboards for a centralized view of Client Third Party Suppliers Information Security posture. Supports Third Party Information Security Risk Reporting, Assessment, and Mitigation. Manage and supports risk based projects from conception through implementation for CITI’s Global Information Security Team. Provide major input on from a security standpoint within the organization’s global security initiatives.

* Create a consolidated view of Citi Third Party Supplier information systems that store, process, and transmit Citi data across its global network through the creation of a consolidated risk dashboard.
* Provides Senior Management with metrics and measurements they need to gain assurance that Third Party Supplier information systems are secure while data is in transit.
* Developing processes and tools for creation for an Information Security Risk Management dashboard to centralize third party suppliers’ information security posture.
* Conducts information security (IS) project planning and scope for Third Party/PCI based information systems for CITI’s facilities globally. Interpreted computer intrusion analysis of suspicious IP addresses
* Provide other line functions with specific information about the operation and effectiveness of particular aspects of information security for which they are responsible (i.e. 3rd Party Citi Connectivity).
* Drive efficiency and improve reporting productivity through the effective use of System Security Plans, Risk Assessments, and Vulnerability Reports. Created information security documentation to develop logical conclusions and to produce technical assessments of Third Party Vulnerability products.
* Conducts information assurance based on PCI requirements under guidance of federal laws such as the Gramm Leach Bliley Act, Sarbanes Oxley, and other international laws to ensure investors’ data is protected.
* Work with system owners, senior management, and other stake holders to determine functionality and usability of generated risk analysis reports for vulnerability management.
* Coordinating and maintaining information security applications: CSI, CASP, AVA, C3PAR, TPAQ. Analyzing new technology transferring protection, emerging technologies, and systems vulnerabilities.
* Collaborates with systems administrators in implementing corrective actions required as result of vulnerabilities uncovered during system scans in coordination with Information Assurance Manager (IAM) and IA Program Manager Guidelines.
* Interfaced with cross functional teams to create potential mitigation solutions for risk areas and track them to resolution. Created Plans of Actions and Milestones to continuously monitor non-mitigated findings.
* Assessed Third Party Supplier’s information security risk posture to ensure compliance with Federal regulations, guidelines, and industry best practices.

**Ketrica R Green Page Four**

**AAFES**, Dallas, Texas **Jun 2013– JUL 2014**

**Sr. Information Assurance Engineer**

Develop and update C&A security artifacts for Army and Air Force retail facilities. Develop security plans, contingency plans, risk assessments, privacy impact assessments, incident response plans, configuration management plans, configurations checklists, and interconnection security agreements for government information security projects while serving as a liaison between the vendor and information security and governance department.

* Performed system development and production documentation of the organizational certification and accreditation process involving security plans and contingency operations (CONOPS).
* Prepared system security profiles that outlined C & A requirements for systems certification
* Conducts and creates risk assessments for MAC III PCI based information systems.
* Conducts the creation on Privacy Impact Assessments for government systems.
* Collaborates with systems administrators in implementing corrective actions required as result of vulnerabilities uncovered during system scans in coordination with Information Assurance Manager (IAM) and IA Program Manager Guidelines.
* Conducts information security (IS) project planning and scope for HIPAA/PCI based information systems for Army and Air Force Retail facilities globally.
* Utilize standard software tools to conduct vulnerability scans of all equipment on the network for vulnerabilities to ensure sound security configurations
* Provide security analysis and C&A/DIACAP support for Enterprise wide IT C&A to include: Datacenter C&A, Enterprise Network Device C&A, and Enterprise Services/Application C&A
* Conducts certification and accreditation of PCI based retail systems to ensure its protective posture in accordance with PCI/PII based standards of operating procedures
* Provide Information System Security Engineering and Certification and Accreditation (C&A) in accordance with DIACAP procedures and guidelines outlined in NIST 800-53.
* Documents project plans for certification and accreditation projects

**DVA**, Austin, Texas **Jun 2011– Mar 2013**

**Sr. Information Assurance Analyst**

Develop and update C&A security artifacts such as security plans, contingency plans, risk assessments, privacy impact assessments, incident response plans, configuration management plans, and configurations for HIPAA based systems that contained data at rest, protected health information, and personal identifiable information.

* Conducts and prepares Systems Security Profiles and Configuration Management Plans detailing probable risks and vulnerabilities associated with information systems, networks, hardware, and software.
* Reviews feedback from customers, complies and analyzes support documents, and recommends procedural changes to information systems to be accredited under the National Institute of Standards and Technology regarding Authorization and Accreditation Process.
* Conduct countermeasure tactics utilizing digital forensics tools against cyber threats while mitigating threats against government information systems by performing risk analysis and assessments to identify threats and vulnerabilities to the private LAN.
* Interfaced frequently with project managers, and customers to provide internal/external audit support involving newly implemented software applications and information systems.
* Established work priorities by severity of incident using risk matrices and impact on business operations.
* Assisted and Guided subordinate organizations in performing tailored assessment during all phases of the (C&A) process to ensure that major systems and applications were ready for certification.

**Ketrica R. Green Page Five**

**STG**, Fort Hood, Texas **Nov 2010 – May 2011**

**Information Assurance Manager**

Support the Modeling, Simulation, and Instrumentation Systems (MS&I).Provide technical security expertise in planning, preparing, and coordinating the Department of Defense (DOD) Information Assurance

Certification and Accreditation Process

* Conducts and prepares Systems Security Tests and Evaluation Plans (ST&EP) detailing probable risks and vulnerabilities associated with Department of Defense Information Systems.
* Reviews feedback from customers, complies and analyzes support data, and recommends procedural changes to information systems to be accredited under the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).
* Conduct countermeasure tactics utilizing digital forensics tools against cyber threats while mitigating threats against the Government Information Grid (GIG) utilizing protocol analyzers and scanners such as Retina and Paraben Forensics Toolkit.

**CDM Solutions**, Killeen, Texas **DEC 2009 – AuG 2010**

**Sr. Information Technology Security Specialist**

Managed and performed security engineering analysis, risk analysis, and vulnerability studies on systems and applications under development by the Department of Defense. Performed systems/software certification and accreditation planning, testing, and risk mitigation to ensure best business practices (BBPs) throughout the entire certification and accreditation (C&A) process.

* Recommended Certification and Accreditation decisions based on severity and impact codes utilizing risk management techniques recommended by the (FISMA) Federal Information Security Management Act.
* Reviews Information Assurance (IA) controls for reaccreditation of existing Department of Defense Information Systems to ensure National Institute of Standards and Technology (NIST) compliance.
* Formulates operational concepts, performs mission, functional analyses, and conducts requirements and information analysis, to determine cost-benefit. Conduct system trade studies, to be utilized during risk management and vulnerability assessments of Government Information Systems (GIS) and networks.

**United States Army** (**Hon. Discharge, DV)**, Fort Hood, Texas **NOV 1998 –MAY 2006**

**Information Assurance Security Officer (IASO)**

Provided security of DOD assets and sensitive personnel information in the fight against terrorism in the support of Operation Iraqi Freedom.

* Conducted system vulnerability and patch management using automated tools and scripts.
* Installed a varied amount of wire, cable, and Ethernet extenders to include routers and hubs.
* Developed and maintained an organization system-level IA program that identified IA architecture, IA requirements, IA objectives and policies.
* Conducts and prepares Systems Security Tests and Evaluation Plans (ST&EP) detailing probable risks and vulnerabilities associated with Department of Defense Information Systems.
* Reviews feedback from customers, complies and analyzes support data, and recommends procedural changes to information systems to be accredited under the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP).
* Conduct countermeasure tactics utilizing digital forensics tools against cyber threats while mitigating threats against the Government Information Grid (GIG) utilizing protocol analyzers and scanners such as Retina and Paraben Forensics Toolkit.

**Ketrica R. Green Page Six**

**Certifications**

|  |
| --- |
| * Certified Information Systems Security Professional (CISSP) Course, October 2016 * Security +, December 2010 * Information Assurance Security Officer Course, October 2016 * DOD DIACAP, December 2016 * Retina Enterprise Suite, November 2016 * Six Sigma (Green Belt Certified), June 2016 * Information Assurance (IAM) Level I/II, November 2016 * HIPAA Training, December 2016 * PCI DSS Certification Course, December 2016 * Privacy Awareness Training, March 2014 * CISSP Training Boot Camp, January 2017 * ITILv3 Training, November 2016 * Microsoft MCSE/MCSA Certification Course, December 2016 * SPLUNK, January 2017 * Project Management Professional (PMP) Course, November 2016 * Forcepoint Websense Administrator, January 2017 * System Administrator/Network Manager -Information Assurance Level II, January 2017 |

**technology**

|  |  |
| --- | --- |
| **Networking / Information Assurance (Ia):** | Cisco Networking, Palo Alto, F5 Networking and Switching Technologies Ethernet, Websense, TCP/IP and DHCP, Telnet, WinSCP, ForcePoint, VMWare ESX, Encase Forensics, Tripwire IDS, SPLUNK, Vulnerability Scanners, Lookingglass, XACTA, VERITAS Backup Exec, and MS SERVER 2012/MIMECAST, and NESSUS. E- Policy SIEM Tools, QRADAR, ARCHER, and McAfee EPO. Oracle IAM UNIX/Linux |
|  |  |
| **Software/Hardware:** | Acronis Imaging Suite, MS SharePoint, Dell Open Manage Software, Visual Basic 2005/ADO.NET 2007, Oracle, Suite/MacAfee, PGP Desktop Encryption, MS Server/Active Directory, PuTTY Telnet Client, Computer Forensics Toolkit, BridgeTrak 8.0 Help Desk Management Suite, I Discovery Asset Management Software, Cisco VPN software, VNC Viewer, F-Secure, Citrix, Paraben Digital Forensics Suite, Encase Forensics. Servers: RAID, PCI, and PCB. Telerik Web Testing/AVA GRC tools. ForcePoint, Digital Guardian, MIMECAST, Palo Alto, Amazon AWS\*f |

**education**

**Masters of Information Technology in Project Management (**11/2010)

American InterContinental University Hoffman Estates, IL

**Bachelor of Information Technology in Computer Forensics (**09/2009)

American InterContinental University Hoffman Estates, IL