PROFESSIONAL SUMMARY

Seasoned professional CRM (Certified Risk Manager) and Project Manager with significant years of project management consulting; analysis and implementation of the NIST Cybersecurity Framework.; ISO 27001 and 27002; Sarbanes Oxley (SOX) Consulting; and auditing experience focusing in Governance Risk and Compliance utilizing the Lock Path version 2 Key light Platform GRC tool; SailPoint IAM Solution Tool; AWS Cloud Security; as well as the RSA Archer Platform GRC tool; Metric Stream GRC Tool; Fiserv Frontier 5.0 tool; Business Intelligence (BI); Project Management, Access Identity Management and Rigorous Program Management. Privileged Access Management; Application Whitelisting; File Integrity Management; Extensive Senior Project Management in Dual Shore Point experience utilizing Waterfall, Agile, as well as Scrum Software Development methodology.

Project Management of AWS Cloud Security; PCI Versions 3.1; 2.0 and Version 1 implementation; Project Manager of major SAP ERP implementation projects (WITH BUDGET IN EXCESS OF $25 MILLION DOLLARS) including SAP Financials (FICO); SAP CRM and SAP SRM Solutions including SAP ECC 5.0 to 7.2; HANA; SAP Warehouse Management Systems. ADP Global Payroll and SOX Compliance Software tools implementation and evaluation. Oracle R12 Implementation and Analysis

Extensive experience in scheduling responsibilities anddeveloping and accurately maintaining integrated master/sub-project schedules, ensuring schedule logic is maintained, coordinating work activities with project team members, progressing schedules and assisting in identifying and resolving schedule conflicts as well as performance of User Acceptance Testing. Extensive experience in analysis and Roll Based Access Control environment and implementation of the NIST Cybersecurity Framework.; Healthcare HIPAA, compliance and development of Standards and Guidelines to adhere to the NIST -800-53, ISO 27001, PCI, ISO 27002, SOX, ADP Global Payroll, Dodd Frank Act, HITRUST; The Volcker Rules; Meaningful Use Act and Sunshine Act requirement and compliance. Extensive experience in AWS Cloud Security; Compliance to NERC Version 3 and 5.1 thru 5.4; PCI Version(s) 2 and 3 Standards and implementation and performance of Compliance QSA Auditing. Extensive experience in IT Technical and Functional requirements to fit client’s needs to meet responsibilities for compliance in NIST; PCI; ISO; HIPAA; HITECH and **other regulatory** Cybersecurity Framework. Compliance to the NEW YORK CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.

TECHNICAL EXPERIENCE

* Project Manager in PCI version 3.1; PCI version 2;SAP ECC 7.2; 7.0;, SAP HANA; SAP COTS packages SAP ECC 5.0 Business One and SAP ECC 6.0 R/3 Functional Conversion; ISO 27001 and 27002; Roll Based Access Control environment; AWL; FIM; PAM; NERC 3 and 5.1; LockPath Keylight GRC version 2; SailPoint IAM Solution Tool; AWS Cloud Security; RSA Archer GRC tool; MetricStream GRC Tool; ControlCase GRC Scan; Qualys Scan; Qualys Guard PCI Scan; PCI ASV Scan; ClearScan; ProCheckUp ASV; Nexus Scan; Nixu Watson Scan Fiserv Frontier 5.0 tool; Oracle R12 Implementation and Analysis; SAP Archiving; ERP; SDLC; Microsoft-Project 2007; IBM Web-Sphere MQ Series; 2003; 2002; and 2000; Access; Oracle R8 thru R12 Financials; SSAE 16 ; SAS 70; Microsoft SharePoint and Microsoft SQL Server; Business Intelligence; Hyperion Financials; ADP Global Payroll; JAVA; DIBS G/L; PRIMAVERA 5.0/8.0/9.1; Vitech (V3)Microsoft VISIO; Excel; Word; Power Point; Lotus Notes; Windows; MS-DOS; HP PPM; RUP; Waterfall, Agile, Scrum Software Development methodology; EDSNET; Win stub; Lotus 123; COBOL; FORTRAN; PL1

PROFESSIONAL EXPERIENCE

LYNX Technology partners, New York, NY March 2017 – Current

**Contracted Certified Risk Management Officer/Security Consultant**

**Clients: (RFQ’s for Various based on bidding Process**)

Contracted Senior Business Consultant with functional responsibility to assist in the development of Statement of work and/or RFQ to coordinate and test IT corporate policies and procedures to meet Federally Regulated NIST Standards and mandated Systems Security Standards for compliance in NIST -800-53, SOX, SAP; PCI; RSA Archer 5.0; MetricStream GRC Tool; Meaningful Use; and Sarbanes Oxley. Required enhance Risk Management Certification by obtaining 24 continuing education units (CEU’s) to implement policies and procedures to meet the SOX Compliance; Access and Identity Management; SAP Project Management; PCI; Compliance experience focusing in Governance Risk and Compliance utilizing the Lock Path version 2 Key light Platform GRC tool HITRUST; Meaningful Use Stage 1 and 2); Sunshine Act; Dodd Frank; Sarbanes Oxley; NIST -800-53; ISO 27002, ISO 27001; SSAE 16 Compliance.

* Defined systems and application security baselines based on industry best practices, which efficiently and effectively mitigated risks, while respecting functionality and operational constraints. Monitored AWS Cloud Security compliance with hardening baselines and manage exceptions
* Performed technical security assessments of information systems and applications to identify vulnerabilities and non-compliance with established security standards and recommend effective mitigation strategies. Supported engineering groups with security engineering expertise in the different security domains, such as identification and access management, authentication and authorization, secure design, system hardening, risk management, vulnerability assessment and management, security testing, secure software development. Supported the development and promotion of information security policies, standards, processes and procedures and monitoring compliance to the information security policy framework with a focus on information system security.
* Supported the development of a risk management framework for information system related security risks and manage information system related security risks accordingly
* Evaluated emerging risks and information security technologies to ensure an up-to-date information security risk register and defined and implement effective, state-of-the-art security concepts.

OPEN SKY CoRPORATION , New York, NY March 2016 – Jan 2017

**Senior Global Privacy Project Manager/Senior Business Analyst/Senior Security Consultant**

**Client: ADP Inc.** (March. 2016 – Jan 2017)

Direct focus was on compliance; process flows and functionality within the RSA Archer Modules:

* Specified, implemented and documented information system security Privacy concepts and information security controls for new systems, ADP Global Payroll and operational systems in close collaboration with system owners and engineering groups.
* Delivered information security Privacy support services to architects and system/application engineers by providing clear, concise and constructive recommendations regarding information system and application security.
* Extensive experience in IT Technical and Functional requirements to fit client’s needs to meet responsibilities for Privacy compliance in AWS Cloud; NIST; PCI; ISO; SOX; HIPAA; HITECH and **other regulatory** Cybersecurity Framework
* Assisted architects, system/application engineers in the identification and implementation of Privacy and other appropriate information security controls and hardening of systems to ensure ADP Global Payroll effective safeguarding of Clients information assets. Defined policies, processes, procedures, configuration baselines and guidelines to ensure appropriate security risk management throughout the system life cycle.
* Defined Privacy system and application security baselines based on industry best practices, which efficiently and effectively mitigated risks, while respecting functionality and operational constraints. Monitored compliance with hardening baselines and manage exceptions for ADP Global Payroll systems.
* Performed technical Privacy security assessments of information systems and applications to identify vulnerabilities and non-compliance with established security standards and recommend effective mitigation strategies for ADP Global Payroll. Supported engineering groups with Privacy security engineering expertise in the different security domains, such as identification and access management, authentication and authorization, secure design, system hardening, risk management, vulnerability assessment and management, security testing, secure software development. Supported the development and promotion of information security policies, Roll Based Access Control environment standards, processes and procedures and monitoring compliance to the information security policy framework with a focus on information system security.
* Supported the development of a Privacy risk management framework for information system related security risks and manage information system related security risks accordingly
* Evaluated emerging risks and information Privacy security technologies to ensure an up-to-date information security risk register and defined and implement an effective, state-of-the-art Privileged Access Management security concepts.
* Supported the development and maintenance of Client’s information security awareness program and training program with content dedicated for system engineers to ensure consistent management of information system security risks.
* Researched and Established the list of Banks and companies that must comply with AWS Cloud and Compliance to the NEW YORK CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES.

OPEN SYSTEMS Consulting, New York, NY December 1 – Feb, 2016

**Senior Global Privacy Project Manager/Senior Business Analyst/Senior Security Consultant**

**Client: AIG International Global Development** (Dec. 1 – February 15)

Direct focus was on compliance; process flows and functionality within the RSA Archer Modules

* Designed, implemented and documented Global information security systems and controls (e.g., file server encryption, SOX, PCI, endpoint security, vulnerability and compliance management solution, security information and event management).
* Lead Global information security projects as laid down in client’s information security (RSA Archer) strategy and recommended a Privileged Access Management (SailPoint IAM Solution Tool) as a projected tool to satisfy identified strategy in the Roll Based Access Control environment.
* Defined, optimized and executed the vulnerability and patch management process. Developed reports from vulnerability assessment scanners, patch management tools, and emerging threat information, advised on the risk remediation and monitored the mitigation of identified security issues.
* Supported security monitoring and security incident responses with a focus on the implementation of effective preventive system security controls as well as containment, eradication and recovery of information systems.
* Assessed system and application security requirements, threats, vulnerabilities and security risks in complex, heterogeneous systems and throughout their life cycle specifically in Global Payroll.
* Developed, delivered and maintained comprehensive and consistent security solutions to mitigate identified risks to an acceptable level.
* Specified, implemented and documented information system security concepts and information security controls for new systems and operational systems in close collaboration with system owners and engineering groups.
* Delivered information security support services to architects and system/application engineers by providing clear, concise and constructive recommendations regarding information system and application security.
* Extensive experience in IT Technical and Functional requirements to fit client’s needs to meet responsibilities for compliance in AWS Cloud; NIST; PCI; SOX; ISO; HIPAA; HITECH and **other regulatory** Cybersecurity Framework
* Assisted architects, system/application engineers in the identification and implementation of PCI, SOX and other appropriate information security controls and hardening of systems to ensure effective safeguarding of Clients information assets. Defined policies, processes, procedures, configuration baselines and guidelines to ensure appropriate security risk management throughout the system life cycle.
* Defined system and application security baselines based on industry best practices, which efficiently and effectively mitigated risks, while respecting functionality and operational constraints. Monitored AWS Cloud Security compliance with hardening baselines and manage exceptions
* Performed technical security assessments of information systems and applications to identify vulnerabilities and non-compliance with established security standards and recommend effective mitigation strategies. Supported engineering groups with security engineering expertise in the different security domains, such as identification and access management, authentication and authorization, secure design, system hardening, risk management, vulnerability assessment and management, security testing, secure software development. Supported the development and promotion of information security policies, standards, processes and procedures and monitoring compliance to the information security policy framework with a focus on information system security.
* Supported the development of a risk management framework for information system related security risks and manage information system related security risks accordingly
* Evaluated emerging risks and information security technologies to ensure an up-to-date information security risk register and defined and implement effective, state-of-the-art security concepts.
* Supported the development and maintenance of Client’s information security awareness program and training program with content dedicated for system engineers to ensure consistent management of information system security risks.

MSH GROUP Consulting, Fort Lauderdale, FL September 15 – November 2015

**Senior Project Manager/Business Analyst/Senior Security Consultant**

**Client: Office Depot/Office MAX** (September 15 – November 2015)

Direct focus was on compliance; process flows and functionality within the RSA Archer Modules

* Senior Project Manager/Business Analyst with functional responsibilities in Implementation, testing and verification of the PCI Version 3.1 DSS Requirements and Mitigating Controls. Project Management, Implementation and Compliance oversite for 8 Major Mitigating Controls and testing of security, risk and compliance management solutions for business acceleration including managing organizational risk, safeguarding mobile access and collaboration, proving compliance, securing virtual and cloud environments, and access and identity management within the Roll Based Access Control environment.
* The Eight targeted areas were:
  + Application Whitelisting
  + Firewall Integrity Management
  + Two Factor Authentication (2FA)
  + Optimize Firewall Rule
  + Enhanced Vulnerability Mitigation Deployment
  + AWS Cloud Compliance
  + Advanced Persistent Threat Defense (APT)
  + Data Loss Prevention (DLT)
  + Privileged Account Management (PAM) (SailPoint IAM Solution Tool)

LYNX Technology partners, New York, NY May 11 – September 2015

**Certified Risk Management Officer/Security Consultant**

**Senior IT Compliance Manager, and Systems Security Subject Matter Expert**

**Client: Crystal Run Healthcare Corporation Inc.** (July 2014 – July 2015)

**(CAP Gemini Corp to Corp)**

* Established the Controls Excellence Program for end-to-end business process as the Business Process Cycle.
* Led, participated as part of the core Controls Excellence management team focused on managing & leading strategic initiatives for Controls Excellence which increase value to the company and partner with leadership to influence and contribute to a strong optimal controls environment which addressed SAP, IT Compliance in SOX, PCI, HIPAA, HITECH reporting requirements, regulatory requirements and standalone reporting requirements.

* Supported leadership in preparing & reviewing deliverables, reports & presentations to Senior Leadership, including the Audit Committee
* Partnered with Controls Excellence Director and provided support in achieving overall goals and metrics of Controls Excellence, including supporting regular dashboard and Steering Committee requirements
* Participated in setting and achieving Access and Identity Management performance metrics and experience focusing in RSA Archer Governance Risk and Compliance utilizing the Privileged Access Management (SailPoint IAM Solution) Tool
* Led, coached and developed resources to achieve the function’s objectives, including their longer-term career aspirations
* Led, motivated and developed the Controls Excellence Team to prioritize and allocate work in order to complete the review, documentation, and testing of key IT and financial business processes to support the Company’s senior management’s SOX, PCI, HIPAA, HITECH and analysis and implementation of the NIST Cybersecurity Framework.; attestation responsibilities and meet other key Controls Excellence strategic objectives and AWS Cloud.
* Identified, managed and reported on all internal control deficiencies real-time and work with business Process Owners to facilitate the creation of action plans and remediation timetables to correct the deficiencies noted.
* Promoted the philosophy of collaborative team working environment, team development across all activities, and focused on the design of new and improved processes in order to achieve business objectives and continuously improve performance within the Controls Excellence Team.
* Partnered with business units and management to foster an environment whereby Controls Excellence was a strategic controls advisor to the organization and helped management effectively manage key IT, financial & regulatory reporting risks
* Worked effectively with key stakeholders, including external auditors and senior management, to promote alignment across understanding of Key Controls and managing expectations.
* Provided the technical and operational expertise and support to all levels of management for compliance with the Sarbanes-Oxley Act, PCI, HIPAA, HITECH and pronouncements of the Public Company Accounting Oversight Board (PCAOB) and the SEC.

**Project Manager, Senior Business Security Analyst, RSA Archer and PCI Compliance and Systems Security Subject Matter Expert**

**Client: Stony Brook University (State of New York)** (March 2014 – July 2014)

**Client: Sherwin Williams Corp. (CAP Gemini Corp to Corp)** (December 2013- March 2014)

**Client: Michigan State University (CAP Gemini Corp to Corp)** (May 2013- November 2013)

* Senior Project Manager/Business Analyst functional responsibility was in Implementation, testing and verification of the PCI Version 2.0 DSS and RSA Archer 5.4 Requirements Implementation and Compliance testing of security, risk and compliance management solutions for business acceleration including managing organizational risk, safeguarding mobile access and collaboration, proving compliance, securing virtual and cloud environments, and access and identity management.
* Primary areas of focus was
  + Platform point of consolidation for governance,
  + Analysis and implementation of the NIST Cybersecurity Framework.
  + risk and compliance information of all types
  + Access and Identity Management Program development and enhancement
  + seamless integration of data systems without the need for additional software
  + Automated movement of data into and out of the Platform to support data analysis
  + Process management and reporting.
  + Governance Risk and Compliance utilizing the Privileged Access Management (SailPoint IAM Solution Tool)
  + Data Feed Manager.
  + Flexible, code-free tool for consolidating information within the RSA Archer eGRC Platform
  + Data Publication Manager which allowed users to automatically extract information from the Platform and load it into external systems for advanced data analysis and modeling
  + Web Services API which supported integration with other business systems using the industry standard SOAP protocol.
  + User and Group Synchronization which supported Active Directory and lDAP integration of user accounts and groups.

The above functions were performed in all of the below RSA Modules:

RSA Archer e-GRC Platform v5.4.4

* [Modules](http://www.emc.com/security/rsa-archer.htm#!modules)

[Policy Management](http://www.emc.com/security/rsa-archer/rsa-archer-policy-management.htm)

[Risk Management](http://www.emc.com/security/rsa-archer/rsa-archer-risk-management.htm)

[Compliance Management](http://www.emc.com/security/rsa-archer/rsa-archer-compliance-management.htm)

[Enterprise Management](http://www.emc.com/security/rsa-archer/rsa-archer-enterprise-management.htm)

[Business Continuity Management](http://www.emc.com/security/rsa-archer/rsa-archer-business-continuity-management.htm)

[Vulnerability Risk Management](http://www.emc.com/security/rsa-archer/rsa-archer-vulnerability-risk-management.htm)

[Security Operations Management](http://www.emc.com/security/rsa-archer/security-operations-management.htm)

[Incident Management](http://www.emc.com/security/rsa-archer/rsa-archer-incident-management.htm)

[Threat Management](http://www.emc.com/security/rsa-archer/rsa-archer-threat-management.htm)

[Vendor Management](http://www.emc.com/security/rsa-archer/rsa-archer-vendor-management.htm)

[Audit Management](http://www.emc.com/security/rsa-archer/rsa-archer-audit-management.htm)

[Federal Assessment & Authorization](http://www.emc.com/security/rsa-archer/rsa-archer-assessment-authorization.htm)

[Federal Continuous Monitoring](http://www.emc.com/security/rsa-archer/rsa-archer-continuous-monitoring.htm)

[GRC Platform](http://www.emc.com/security/rsa-archer/rsa-archer-egrc-platform.htm)

**Clients: (Various**) **(September 2012- May 2013)**

Senior Business Analyst where functional responsibility was to assist in the development of Statement of work and/or RFQ to coordinate and test IT corporate policies and procedures to meet Federally Regulated NIST Standards and mandated Systems Security Standards for compliance in NIST -800-53, SOX, SAP; PCI; RSA Archer 5.0; MetricStream GRC Tool; Meaningful Use; and Sarbanes Oxley. Required enhance Risk Management Certification by obtaining 24 continuing education units (CEU’s) to implement policies and procedures to meet the SOX Compliance; Access and Identity Management; SAP Project Management; PCI; Compliance experience focusing in Governance Risk and Compliance utilizing the Lock Path version 2 Key light Platform GRC tool HITRUST; Meaningful Use Stage 1 and 2); Sunshine Act; Dodd Frank; Sarbanes Oxley; NIST -800-53; ISO 27002, ISO 27001; SSAE 16 Compliance.

* + Governance Risk and Compliance utilizing the Privileged Access Management (SailPoint IAM Solution Tool)
  + Data Feed Manager.
  + Flexible, code-free tool for consolidating information within the RSA Archer eGRC Platform

**Project Manager, Senior Business Security Analyst, RSA Archer Systems Security Implementation**

**Client: Accuride Corporation (IBM Corp-to-Corp**) **(February 2012- August 2012)**

Senior Business Analyst where functional responsibility was to develop, coordinate and test IT corporate policies and procedures to meet Federally Regulated NIST Standards and mandated Systems Security Standards for compliance in SAP 7.0 to 7.2 HANA environment. Helped to implement policies and procedures to meet the Sarbanes Oxley; NIST -800-53; ISO 27002, ISO 27001; SSAE 16 Compliance;

* Senior Project Manager/Business Analyst functional responsibility was in Implementation, testing and verification of the PCI Version 2.0 DSS and RSA Archer 5.2 Requirements Implementation and Compliance testing of security, risk and compliance management solutions for business acceleration including managing organizational risk, safeguarding mobile access and collaboration, proving compliance, securing virtual and cloud environments, and access and identity management.
* Primary areas of focus was
  + Platform point of consolidation for governance,
  + Analysis and implementation of the NIST Cybersecurity Framework.
  + Risk and compliance information of all types
  + Seamless integration of data systems without the need for additional software
  + Automated movement of data into and out of the Platform to support data analysis
  + Process management and reporting.
  + Access and Identity Management enhancement
  + Data Feed Manager.
  + Flexible, code-free tool for consolidating information within the RSA Archer eGRC Platform and the Privileged Access Management (SailPoint IAM Solution Tool)
  + Data Publication Manager which allowed users to automatically extract information from the Platform and load it into external systems for advanced data analysis and modeling
  + Web Services API which supported integration with other business systems using the industry standard SOAP protocol.
  + AWS Cloud Security
  + User and Group Synchronization which supported Active Directory and lDAP integration of user accounts and groups.

The above functions were performed in all 14 RSA Archer e-GRC Platform v5.2.4

**Client: Bank of New York Mellon** **(June 11– October 11)**

**Project Manager, Senior Business Analyst, RSA Archer and PCI Security Standards Implementation**

Active Directory and Bind view implementation and testing to ensure compliance to meet Federally Regulated NIST Standards (NIST -800-53) and mandated SOX Systems Security Standards.

Additional responsibilities were penetration testing and verification of the PCI Version 2.0 DSS and RSA Archer 5.0 Requirements developed towards reaching the following six (6) milestones:

* Removing sensitive authentication data and limit data retention.
* Protecting the perimeter, internal and wireless networks.
* Securing payment card applications.
* Monitoring and controlling access to IT financial systems.
* Protecting stored cardholder data.
* Analysis and implementation of the NIST Cybersecurity Framework. experience focusing in Governance Risk and Compliance utilizing the Lock Path version 2 Key light Platform GRC tool
* Finalizing remaining compliance efforts and ensure all controls are in place.
* Vulnerability Management
* Oracle R12 functionality and Compliance Analysis
* Access and Identity Management
* Directly responsible for implementation team of 16
* Compliance Monitoring of implementation of RSA Archer Platform GRC tool
* ISO 27002, ISO 27001; SSAE 16 Compliance
* Change Management Compliance and Process Implementation
* Business Intelligence (BI)
* Monitoring and controlling Identity Management applications access to IT financial systems
* Writing and maintaining process procedures and controls
* Reviewed and improved ADP Global Payroll Standards
* Consulting in the research, design and implementation of The Dodd Frank Act and The Volcker Rules requirements.
* Senior Project Manager/Business Analyst functional responsibility was in Implementation, testing and verification of the PCI Version 2.0 DSS and RSA Archer 5.1 Requirements Implementation and Compliance testing of security, risk and compliance management solutions for business acceleration including managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.
* Primary areas of focus was
  + Platform point of consolidation for governance,
  + Analysis and implementation of the NIST Cybersecurity Framework.
  + risk and compliance information of all types
  + seamless integration of data systems without the need for additional software
  + Automated movement of data into and out of the Platform to support data analysis
  + Process management and reporting.
  + Data Feed Manager.
  + Flexible, code-free tool for consolidating information within the RSA Archer eGRC Platform
  + Data Publication Manager which allowed users to automatically extract information from the Platform and load it into external systems for advanced data analysis and modeling
  + Web Services API which supported integration with other business systems using the industry standard SOAP protocol.
  + User and Group Synchronization which supported Active Directory and lDAP integration of user accounts and groups.

The above functions were performed in all 14 RSA Archer e-GRC Platform v5.2.4

**Client: Disney Corporation World-Wide** **(May 11- January 12)**

Business Analysis where I analyzed documented and published a corporate report on the KMF which focused on issues involving the management of cryptographic keys: their generation, use, and eventual destruction. The final report included related topics, such as algorithm selection and appropriate key size and cryptographic module selection.

* Directly responsible for implementation team of 10
* Oracle R12 Implementation and Analysis
* Compliance to NIST -800-53
* Compliance experience focusing in Governance Risk and Compliance utilizing the Lock Path version 2 Key light Platform GRC tool
* Analysis and implementation of the NIST Cybersecurity Framework.
* Vulnerability Management
* Compliance Monitoring of implementation of RSA Archer Platform GRC tool
* ISO 27002, ISO 27001; SSAE 16 Compliance
* Access and Identity Management
* Writing and maintaining process procedures and controls
* Compliance to NERC Standards
* Business Intelligence (BI)
* Monitoring and controlling Identity Management applications access to IT financial systems Change
* Monitoring and compliance to ADP Global Payroll Standards
* Management Compliance and Process Implementation
* SSAE 16 Compliance

Robert Half Management, Inc, Princeton, NJ Aug 07 – April 11

**Project Manager, Security Standards Implementation**

**Client: Citi Corp Trust Delaware CC Center** **(Feb 10 – Apr 11)**

Responsibilities were penetration testing and verification of the PCI Version 1.0 DSS Requirements developed towards reaching the following six (6) milestones:

* Removing sensitive authentication data and limit data retention.
* Protecting the perimeter, internal and wireless networks.
* Securing payment card applications.
* Monitoring and controlling access to IT financial systems.
* Protecting stored cardholder data.
* Finalizing remaining compliance efforts and ensure all controls are in place.
* Vulnerability Management
* Directly responsible for implementation team of 18
* Consulting in the research, design and implementation of SOX and The Dodd Frank Act and The Volcker Rules requirements.
* Change Management Compliance and Process Implementation
* Analysis and implementation of the NIST Cybersecurity Framework.
* ISO 27002, ISO 27001; SSAE 16 Compliance
* Business Intelligence
* Monitoring and controlling Identity Management applications access to IT financial systems
* Writing and maintaining process procedures and controls
* Compliance Monitoring of implementation of the Fiserv Frontier 5.0 tool

**Project Manager, IT Corporate SOX Compliance**

**Client: EPV SOLAR, Inc., Robbinsville, NJ** **(Aug 07 – Dec 09)**

* Project Manager SOX Compliance and Senior SAP Subject Matter Expert responsible for the IT System transition from E-Synergy to the COTS package SAP ECC 6.0 R/3 ($6 million dollar budget). Responsible for the successful planning and execution of the SAP Archiving, conversion and implementation project including defining project approach and gaining client, client engagement manager and project team member’s buy-in for 28 Solutions including SAP Financials (FICO) SAP CRM and SRM Solutions including SAP HANA environment.
* Dual Shore point responsibility managing the custom built combination of the best local and off-shore talent to bring the client the highest quality
* Change Management Compliance and Process Implementation
* Analysis and implementation of the NIST Cybersecurity Framework.
* Vulnerability Management
* Writing and maintaining process procedures and controls
* ISO 27002, ISO 27001; SSAE 16 Compliance
* Business Intelligence
* Compliance to NERC Standards
* Compliance Monitoring of implementation of RSA Archer Platform GRC tool
* Using Rigorous Program Management/RPM led and directed implementation team of 23 contracted consultants and employees, responsible for the successful implementation of the Business Suite Module. Communicated project status, milestones and issues to project owners.

GRANT THORNTON, Inc, Miami, FL Aug 06 – Aug 07

**Position: Project Manager, IT and SOX Systems Compliance and Testing**

**Client: MIVA, Inc., FT. Myers, FL**

* Senior SOX Project Manager, SAP Project Manager and Subject Matter Expert responsible for the ERP transition from MAS 500 to SAP COTS package SAP ECC 5.0 Business One ($8 million dollar budget). Direct implementation responsibility for the Business Suite Module. SAP Business Suite provided the company with industry-specific applications. Overall responsibility for the successful planning and execution of the SAP project for 24 Solutions including SAP Financials (FICO) SAP CRM and SRM Solutions in the SAP HANA environment.
* Dual Shore point responsibility managing the custom built combination of the best local and off-shore talent to bring the client the highest quality
* Compliance Monitoring of implementation of the RSA Archer Platform GRC tool version 2 Platform GRC tool
* Directly responsible for implementation team of 15 responsible for the Business Suite Module.
* Change Management Compliance and Process Implementation
* Vulnerability Management
* Analysis and implementation of the NIST Cybersecurity Framework.
* ISO 27002, ISO 27001; SSAE 16 Compliance
* Oracle R12 Implementation
* Business Intelligence
* Monitoring and controlling Identity Management applications access to IT financial systems
* Writing and maintaining process procedures and controls around ADP Global Payroll Standards
* Communicated project status, milestones and issues to project owners.

Robert Half Management, Inc, Madison Heights, MI May 06 – Aug 06

**Project Manager, Systems IT Testing and Compliance**

**Client: COMERICA Bank, Auburn Hills, MI**

Enterprise Resources, Inc, Mt. Laurel, NJ Sep 05 – May 06

**Project Manager Sarbanes-Oxley Testing and Compliance**

**Client: Dynamic Details Inc. Anaheim, CA** (Oct 05 – May 06)

**Senior Project Manager, SOX Compliance and Testing**

**Client: Warrick Valley Communications, Inc. Warrick, NY** **(Sep 05 – Oct 05)**

Control Solutions, Inc, New York, NY May 05 – Oct 05

**Senior Executive Consultant/Subject Matter Expert**

**Client: 4 Kids Entertainment, New York, NY** **(May 05 – Aug 05)**

**Senior Executive Sarbanes-Oxley Consultant**

**Client: Atlantic Broadband Cable** (4 offices) Boston, Miami, Pittsburg **(Aug 05 – Oct 05)**

Dickerson Allen, Inc, Troy, MI Jan 05 – Apr 05

**Senior Documentation and Testing Consultant**

**Client: Intermet Manufacturing**, **Troy, MI** **(Feb 05 – Apr 05)**

**Senior Documentation and Testing Consultant**

**Client: Tier Technologies, Vienna, VA** **(Jan 05 – Feb 05)**.

Robert Half Management, Inc, Troy, MI Aug 04 – Oct 04

**Senior Consultant SOX**

**Client: Detroit Diesel Corporation,** **Aug 04 – Oct 04**

**Client: ADP Payroll/Sandy Corporation**, **Oct 04 – Dec 04**

CAP Gemini, Inc., New York, NY Dec 03 – Aug 04

**Senior Consultant, Senior Sarbanes-Oxley Consultant**

**Client: Kaiser Permanente Insurance, Oakland, CA** **(May 04 – Aug 04)**

**Project Manager, Consultant, HIPAA Implementation/Testing**

Client: Binson's Durable Medical Equipment Warren, MI (Dec 03 – Apr 04)

Iconmi, Inc, Troy, MI Feb 03 – Nov 03

**Senior Business Analyst/HIPAA Implementation/Testing**

**Client: Cigna Healthcare, Hartford, CT**

Marsh & McLennan Inc., ST. Louis, MO Jan 02 – Jan 03

**Project Manager, Lead Business Analyst/HIPAA Implementation**

CAP Gemini, Inc, New York, NY Jun 01 – Dec 01

**Project Manager, HIPAA Compliance Coordinator, HIPAA Implementation/Testing**

**Client: Lutheran Social Services of Michigan**

DPM Consulting, Inc, Troy, MI Jun 96 – May 01

**Senior Consultant/ Senior Auditor**

**Client: General Motors Corporation, Detroit, MI**

**Directly assigned to Blue Cross Blue Shield Michigan**

EDUCATION

**Bachelors of Science, Business Administration (1973)**

**Specialization Accounting/Mathematics**

Bethune-Cookman College, Daytona Beach, Florida

TRAINING AND CERTIFICATION

**Certified Risk Manager**

Certified in Risk Management (CRM), April 2008

CEU focus in Project Management of SAP Security and Risk April 2009

CEU focus in Payment Card Industry version 2.0 Data Security Standard (PCI DSS) November 2010

CEU focus on NIST Security and Compliance Standards November 2011

CEU focus on NIST -800-53; ISO 27001 through ISO 27006 November 2012

CEU focus on The Dodd Frank and Volcker Rule Compliance and Implementation January 2013

CEU focus on SAP Accelerated Implementation Program February 2013

CEU focus on SRM SAP Implementation and Testing March 2013

CEU focus on CRM SAP Implementation and Testing April 2013

CEU focus on Oracle R12 Implementation, Compliance and Testing May 2013

CEU focus on The Sunshine Act Reporting and Compliance September 2013

CEU focus on ICD 10 Implementation and Compliance December 2013

CEU focus on PCI Version 3.0 Changes and Compliance July 2014

CEU focus on SAP GRC 10.1 Implementation and Compliance July 2014

CEU focus on SAP Identity Management Implementation February 2015

CEU focus on Access and Identity Management Implementation and Testing March 2015

CEU focus on PCI Version 3.1 Changes and Compliance July 2015

CEU focus on Risk Management (VECTOR Matrix) Self-Assessment Security Risk July 2016

CEU focus on Risk Management (OCTAVE Method) Self-Assessment Security Risk August 2016

CEU focus on Advance Compliance to AWS Cloud Security February 2017

CEU focus on AWS Cloud Security Risk March 2017

**Institute of Internal Auditors**

Certified, Health Care Internal Auditor, March 1986

One of only 965 Auditors inducted into the Healthcare Internal Audit Group

**American Management Association**

Completed more than 35 CPE hours in various Executive Management Programs and seminars.

Completed the Sarbanes-Oxley training in September 2003