

**RICARDO RODRIGUEZ****INFORMATION SECURITY, RISK, AUDIT & COMPLIANCE**(267) 949-7046 [RICARDORODZ12@YAHOO.COM](mailto:RICARDORODZ12@YAHOO.COM)

Motivated, detail-oriented, and dynamic professional with more than 20 years of experience in designing/implementing information systems, leading and designing diverse cyber security, internal, finance, regulatory compliance, investment advisory/company reviews, and information security audits in banking, financial, governmental, utilities, and not-for-profit industries. Employers included: Securities and Exchange Commission, Federal Reserve Bank of Philadelphia, ING Financial Services Company, Capmark Bank, GlaxoSmithKline Pharmaceuticals, NRG Energy, Inc., PJM Interconnection LLC., and U.S. ARMY. Areas of Expertise include:

- ✓ Information Security, Cyber Security, HIPAA, PCI, SOX, PII, and Privacy Laws, Cloud and Vendor Risk Management
- ✓ NERC CIP & 693 Compliance, SCADA Systems Security Reviews
- ✓ Policy Development and Compliance
- ✓ Excellent Teamwork Skills
- ✓ Federal & State Regulations
- ✓ Team Leadership & Training
- ✓ GDPR, FCPA, DoD, B2B/B2C, e-commerce Reviews
- ✓ Intrusion detection/prevention systems, Incident Response
- ✓ Davis Beacon & DOE Compliance
- ✓ Access Management, Network Security, Excellent Project Management Skills
- ✓ GLBA Security & Risk Assessments
- ✓ Auditing & Compliance Standards
- ✓ Internal Audit and Risk Management
- ✓ SCADA Compliance Audits
- ✓ SEC Investment Advisory and Investment Company Reviews
- ✓ Financial Services Compliance
- ✓ FFIEC, SOX, SOC 1&2 Reviews
- ✓ Cloud Governance Compliance and Practices
- ✓ Mobile and Wireless Security
- ✓ Strong Leadership Skills
- ✓ Risk Management Methodologies
- ✓ NIST 800-53, ISO27001/27032, COBIT, COSO, FINRA, FISMA

## EDUCATION & QUALIFICATIONS

### Graduate Certificate in Cybersecurity

Rutgers University – New Brunswick, NJ – 2019

### Master of Science in Engineering (MSE), Technology Management

UNIVERSITY OF PENNSYLVANIA | Philadelphia, PA | 2003

**Bachelor of Business Administration**, Computer Information Systems, University of Puerto Rico – San Juan, PR

### Professional Certifications:

Certified Information Systems Auditor (CISA) | Certified Information Security Manager (CISM)  
 Certified ISO27001 Lead Auditor | Certified ISO27032 Lead Cyber Security Manager | CompTIA Security+  
 Certified SCADA Security Architect (CSSA) | Certified Computer Forensics Examiner (CCFE)  
 Certified Internal Controls Auditor (CICA) | Certification in Risk Management Assurance (CRMA)

## PROFESSIONAL EXPERIENCE

### PJM INTERCONNECTION LLC • Norristown, PA • 2012 – Present

#### CHIEF AUDIT & COMPLIANCE EXECUTIVE

#### KEY ACCOMPLISHMENTS:

- Lead an internal team in performing and reviewing all finance, information security, regulatory, compliance, regulatory, cyber security, operational, information systems, vendor risk management, FCPA, GDPR, and information security reviews.
- Perform ongoing risk assessments and continually update or revise audit and compliance plan based on performance and emerging threats to proactively monitor and mitigate risks and evolving needs.
- Ensure continuous improvement and ongoing compliance through creation, enforcement, and training in all Information Security, NERC CIP, Physical Security, OSHA, BCP/DR policies.

**PROFESSIONAL EXPERIENCE, CONTINUED**

- Implementation and evaluation of Information and Cyber Security Program and controls.
- Provide information and cyber security guidance and training to employees and stakeholders in the program.
- Established readiness and knowledge successful in implementing and achieving NERC CIP/FERC, ISO27001, ISO27032, and SCADA and SOC1 compliance certifications.
- Serve as Vendor Security Reviews, Information Security & Records Retention Champion.
- Oversee Cloud Governance Committee responsible for evaluating and selecting cloud solutions.
- Responsible for administering PJM's Ethics Hotline and coordination of reported incident investigations.
- Lead Member of Incident Response and Pandemic Team.
- Work with Technology Department and other business unit stakeholders during project and product development efforts to ensure that appropriate security controls are considered during system/application implementations, vendor selection, and policy development.
- Perform periodic access controls reviews, report on issues identified, and work with management to identify solutions and mitigation plans.
- Manage a team of 8 internal employees and a team of 20 external auditors.
- Provide regular reports and status updates to Audit Committee, Board of Managers, and Executive Management.
- Member of Executive Leadership Team.
- Role reports to CEO and Board of Managers.

**NRG ENERGY, INC. • Princeton, NJ • 2010 – 2012****DIRECTOR OF COMPLIANCE, FINANCIAL AND INFORMATION SECURITY AUDITS (2010 – 2012)****KEY ACCOMPLISHMENTS:**

- Directed an internal team in performing and reviewing all information security, regulatory, compliance, regulatory, cyber security, operational, financial, information systems, vendor risk management, FCPA, GDPR, and information security reviews.
- Ensured continuous improvement and ongoing compliance through creation, enforcement, and training in all information and cyber security, financial, and internal security policies.
- Responsible for risk assessment and evaluation of security controls including access controls, development and monitoring of policies and standards, security awareness, project and product development consultation, incident response program management, and ongoing compliance with industry regulations related to information security.
- Performed information & cyber security risk management tasks and evaluated information & cyber security program controls.
- Built and leveraged relationships with External Auditors to collaborate on all audits and diverse projects.
- Earned promotion after less than one year with company based on exceptional aptitude for leadership, outstanding performance, and proven knowledge of audit methodologies and regulations.
- Performed fraud investigations as needed, leveraging in-depth knowledge of regulations and compliance laws.
- Evaluated and adjustment annual audit plans and strategies based on annual IT risk assessment.
- Managed a team of 7 internal employees and 15 external auditors.

**Capmark Bank • Horsham, PA • 2008 – 2010****VICE PRESIDENT OF GLOBAL CYBER & IT SECURITY****KEY ACCOMPLISHMENTS:**

- Responsible for risk assessment and evaluation of security controls including access controls, development and monitoring of policies and standards, security awareness, project and product development consultation, incident response program management, and proactive compliance with industry regulations related to information security.

**PROFESSIONAL EXPERIENCE, CONTINUED**

- Developed and implemented information security policies and standards, in conjunction with the Technology Department and other stakeholders.
- Performed cyber security risk management tasks and evaluated cyber security program controls.
- Built and launched and IT compliance department from ground up including security policy design and training, subsequently achieving organizational compliance with Sarbanes Oxley regulations, FFIEC and FED regulations.
- Successfully maximized utilization of resources in collaboration with Internal and External auditors.
- Proactively identified and developed solutions to Information Security and IT risks, cyber security, compliance, and execution for Capmark Bank servicing U.S., Japan, and Ireland.
- Managed a team of 10 internal employees and five external contractors.

**GLAXOSMITHKLINE (GSK) • Philadelphia, PA • 2004 – 2008****IT AUDIT & SECURITY MANAGER****KEY ACCOMPLISHMENTS:**

- Executed and evaluated all phases of audit planning and performance for technology, cyber and information security, Vendor Security, FCPA, and financial controls in domestic and international operations. Oversaw SAP/ERP implementation both nationally and globally.
- Provided security consulting on best practices for infrastructure and network systems (i.e., OS, network, firewalls, routers, switches, IDS, IPS, web server, application server, etc.)
- Worked IT and business unit stakeholders during project and product development efforts to ensure that appropriate security controls were considered during vendor selection and development efforts.
- Designs and conducts information security risk assessments to evaluate inherent risks, controls, and residual risks.
- Works closely with Technology teammates responsible for user security and access controls to review privileged levels of access and changes to the technology environment for risk.
- Monitors emerging threats and recommends mitigation strategies. Oversees security awareness activities for Bank teammates and customers, ensuring that the Bank culture maintains a high commitment to security and regulatory compliance.
- Oversees the incident response process, including but not limited to developing and managing guidelines and proactively identifying and recommending mitigation strategies
- Spearheaded recruitment, coaching, training, and ongoing mentorship of international team of 25 members.
- Earned status as Subject Matter Expert and primary Point of Contact for cyber security, offshore/outsourcing vendor audits.
- Served as Vendor Security Reviews, Information Security & Records Retention Champion.

**ING FINANCIALS • New York • 8/2000 – 8/2004****IT AUDIT & SECURITY MANAGER****KEY ACCOMPLISHMENTS:**

- Responsible for conducting all phases of audit planning and execution for network security, technology, e-commerce, information security and financial audits in both domestic and international operations.
- Member of the Latin America Information Security Group - Group was responsible for security policy creation, enforcement, training, and development of controls for all of Latin American offices (Brazil, Argentina, Mexico, Puerto Rico). Responsibilities also included evaluation of systems/applications that collected, processed and/or stored PII and management and implementation of controls designed to protect sensitive and confidential data.
- Responsible for planning and performing GLBA risk assessments, controls testing, and reporting.
- Participate in Fraud Investigations and Financial Audits (15%)
- Supervision of 13 direct staff members.
- Managed IT budget of approximately \$300 million.

**PROFESSIONAL EXPERIENCE, CONTINUED****FEDERAL RESERVE BANK OF PHILADELPHIA (FED) • Philadelphia, PA • 10/1997 - 8/2000****SENIOR TRAINING AND INTERNAL CONTROLS COORDINATOR (10/1997 - 8/2000)****KEY ACCOMPLISHMENTS:**

- Responsible for aligning the overall business application development strategy with department's business goals and objectives.
- Member of the leadership team responsible for providing ongoing direction and feedback for all business application development initiatives across multiple businesses to meet agreed upon business objectives and financial targets.
- Managed the Security and Information Systems Audit function including quality assurance and security functions for all Cash Services Department computing services to ensure compliance with Federal Reserve Systems regulations.
- Responsible for department's Audit Preparedness Program. The program objective was to conduct mock audits of all (or selected areas based on risk) security, compliance and policy/procedure assessments for the department on a periodic basis looking to examine overall security levels in the environment and in policy/procedural areas to ensure that the required processes were identified, developed, scheduled for implementation and implemented and ensure audit readiness.
- Responsible for the planning and execution of GLBA risk assessments, controls testing, and reporting.
- Responsible for managing department's incident and problem escalation overall efforts. Development and Acquisition, Operations, and E-banking.
- Performed FFIEC review of banking institutions within geographical coverage locations (New Jersey, Pennsylvania, Delaware)
- Responsible for managing training and IT budget.

**UNITED STATES SECURITIES AND EXCHANGE COMMISSION • Washington, DC & Philadelphia, PA • 02/1993 - 10/1997****Senior Internal Auditor (Examiner)****Key Accomplishments:**

- Performed full financial/operational audits of broker dealers, transfer agents, investment advisors, and investment companies.
- Reviewed new system design projects and changes to computer programs to insure adequate controls and audit trails are included. Verified controls and tested the accuracy of automated systems.
- Provided training to new employees on audit and report writing techniques. Direct supervision and training of six staff members.
- Reached career growth upper tier and decided to move for promotion of career to FRB.