NICHOLAS PANDOLA, MBA, CRISC, CISA, QSA, CCNP Greater Philadelphia |
215-809-4447 | npandola79@gmail.com **https://www.linkedin.com/in/pandolanicholas/**

GLOBAL INFORMATION SECURITY LEADER (CISO, IT Director, Security Architect)
A leader that will reduce cybersecurity risks and improve technology maturity. Designed numerous cybersecurity and compliance programs for multinational businesses. Deep understanding of domestic and international technology landscapes, Zero Trust, CIS, Azure hosting, and Defense in Depth. Collaborate on team goals and mentor for efficient problem solving and change agent supporting behavior. Multiple industry backgrounds including chemical, manufacturing, retail, financial and professional services, pharmaceutical, healthcare, consumer goods, and consulting.

Passion for information security, risk management, coaching team members, consistent provider of compliance controls and driver of enterprise-wide information security best practices. Bring a positive attitude to opportunities, is present, and accessible. Earned a reputation for being a proactive, innovative, collaborative, consensus building, inclusive, business leader and partner with excellent presentation, analytical, communications, negotiate, and influence skills. Comfortable delivering results in a cross-functional, fast-paced environment. Ability to work independently and in a team environment.

CORE COMPETENCIES: **Strategic Planning & Execution | Operational Technology (Rockwell, ABB) | New Technologies Evaluation | Risk Management | Technology Audits | Team Training, Mentoring | Security Assessments, Internal, External, 3rd parties | Cost Controls | Data Protection | Incident Management | Budgeting | Vulnerability & Threat Assessment | Information Security Program Development | Stakeholder & Vendors Relations (TPRM) Vendor Management | Compliance Monitoring | Identity & Access Management | Project Management Policies-Procedures-Protocols | Awareness Training | Business Continuity Planning | Contract Negotiating | Metrics/KPIs | Secure Data Management**

CAREER HISTORY

Principal Security Architect, CEDAR GROVE SECURITY ADVISORY LLC, August 2023-present

- Provide a range of contractor services relating to strategic planning, risk management, security program vision and cloud Architecture.

Selected Engagement:

- **Risk Assessment:** Identify the key cyber security risks, build the business case for improvements, formulate corresponding management action plans that close the gaps.
- **Policy and Process:** Review information security policies and SOPs to fit for the business requirements, conduct gap analysis and ensure compliance of industry standards.
- **Project Management:** Developed project implementation schedule for information security program and infrastructure advancements.

CHIEF INFORMATION SECURITY OFFICER (CISO), TRINSEO, January 2018- August 2023
Strategic Leadership: Develop and lead a comprehensive zero trust strategy aligned with business objectives and growth plans that reduced risk by 40% in less than 12 months.

Security Program Development: Set the vision for the establishment and operation of the first security monitoring and threat intelligence programs. Resulted in automation detection to respond to millions of security incidents in real-time.
Selected leader: Critical project to insource Information Security, Hosting, and Infrastructure team, providing clear direction, guidance, and mentorship.
Team Leadership: Designed and identified cross functional team of Information Security and Infrastructure operational management team (26 domestic & global).
Metrics/KPIs: Established monthly metrics and key performance indicators (KPIs) to monitor the effectiveness of the information security program (Incidents Managed, Risks mitigated, Projects completed, Open risks and controls).
Hosting Migration: Review and evaluation of cloud services, including proper sizing, RI, and identification of correct MS services and Azure region. Migrated two data centers and OT DevOps to Azure East 2 and AzureGermany.
Budget Management: Developed and rationalized an operational budget of 15MM. Managed the Azure and Microsoft budget of 3MM, security and compliance requirements of 3MM, capital budget of 4MM. Solved a shortfall by implementing an in-sourcing model for the Infrastructure services.
Risk Assessments: Identified vulnerabilities, threats, and risks to the information systems, networks, and security program. Including risk mitigation strategies, threat Intelligence frameworks including controls, safeguards, and incident response plans, to protect against unauthorized access, data breaches, and cyber threats.
Leadership of Infrastructure Operational Team: including, WAN, LAN, Intune Policies and Procedures, Desktop and Collaboration suites, cloud architecture, cloud security and hosting operations with a focus on resilient environments
Leaderships of the IT compliance Team: associated with SOX, ISO, NIST, and CIS requirements. and to develop a culture of security awareness. Initiate conversations on evolving security best practices, hacking back, threat attribution,DMARC Threats.
Selected Highlights:

- Rapid response: Designed the first information security strategy and road map leveraging zero trust architecture as the bedrock foundation. Using MSSPs and internal team members.
- Operational Technology: Extensive experience collaborating with the process automation team designed a new cybersecurity roadmap, resolved PIM audit findings and critical detection gaps.
- Globalization: Completed the leadership and strategy architecture for moving from 2 on premise data centers to a global Azure design.
- Cost Savings: Collaborated with finance and procurement teams to control costs, evaluate vendor contracts, and identify opportunities for cost savings.
- Resource Optimization: Developed and managed the infrastructure and security budget, optimizing resource allocation to meet the technology needs of domestic and international offices.

CHIEF INFORMATION SECURITY OFFICER, SOLENIS, April 2015 - January 2018
Security Program Development: Completed the establishment and operation of a comprehensive security monitoring and threat intelligence programs to detect and respond to security incidents in real-time.
Metrics/KPIs: Established appropriate metrics and key performance indicators (KPIs) to monitor the effectiveness of the information security program.

Stakeholder Relations: Communicated with executive management and board members, highlighting the security posture, risks, and recommendations for improvement. Collaborated with finance, procurement, and vendors (including sourcing and contract negotiations).
Risk Management: Completed risk assessments to identify vulnerabilities, threats, and risks to the information systems, networks, and security program. Including risk mitigation strategies, threat Intelligence frameworks including controls, safeguards, and incident response plans, to protect against unauthorized access, data breaches,and cyber threats.
Staff Management & Development: Completed leadership for a team of 3 and 2MM operational budget. Applied innovative thinking with an ability to build, lead and motivate cross-functional, interdisciplinary teams. A strong developer of Information Security leaders.
Selected Highlights:

- Designed the first security program and performed network migration after a divestiture.
- Directed a security awareness campaign that presents best practices for protecting consumer and sensitive data.
- Directed a risk management campaign that presents controls for protecting consumer and sensitive data.

SENIOR DIRECTOR CYBER SECURITY, GRANT THORNTON, January 2005 - April 2015
Strategic Leadership: Developed comprehensive security monitoring, compliance management programs and threat intelligence strategies for clients to detect and respond to compliance and security incidents in real-time.
Concept Development: Designed a PCI QSA consulting service, including business case, product management, proposals and rfps templates, focusing on retail and consumer companies.
Risk Management: Completed risk assessments to identify vulnerabilities, threats, and risks to the information systems, networks, and security program. Developed risk mitigation strategies, threat Intelligence frameworks including controls, safeguards, and incident response plans, to protect against unauthorized access, data breaches, and cyber threats.
Audit Reviews: Communicated IT control strengths and weaknesses to the client or internal audit engagement team.
Selected Highlights:

- Security Road Map: Translated strategic requirements into an enterprise information architecture security road map to guide solution development and achieve consistency of information technology compliance strategy.

EDUCATION

Executive MBA, System Operations, VILLANOVA UNIVERSITY
B.S, Accounting, DREXEL UNIVERSITY

CERTIFICATIONS & CREDENTIALS

CRISC – Certified Risk Information Systems Control
QSA – Qualified Security Assessor
CISA – Certified Information Systems Auditor
CCNP – Cisco Certified Network Professional