Ronald Bambot, CISM, PMP

#### SECURITY CLEARANCES: Clearable

#### 

#### EDUCATION:

Mr. Bambot Exceeds minimum requirements for this position as follows:

* Master’s Degree in Cybersecurity
* Over ten (10) years of relevant experience
* Exceptional cyber certifications including CISM and Security+
* Master’s Degree, Cybersecurity, University of Maryland
* Bachelor’s Degree, Bridgewater State University

#### PROFESSIONAL CERTIFICATIONS**:**

* PMP
* CISM
* CompTIA Security+
* Certified Scrum Master
* Linux system
* Aws solution Architect

#### EXPERIENCE SUMMARY**:**

Mr. Bambot is anexperienced, passionate, and goal-oriented Cybersecurity Specialist, with over ten (10+) years of diversified experience in cybersecurity. A team player and problem solver with tested resolve, passion, and creativity in addressing issues related to building Information Technology (IT) network infrastructures and migrations at the enterprise level. Proficient in network architecture protocols, server maintenance, and data communications. He possesses excellent communication and documentation skills in interpreting technical details to non-technical clients and staff. Self-motivated, proactive, and has the ability to thrive in fast-paced, innovative, mission-critical operational environments. He possesses strong IT skills and knowledge including hardware, software and networks and has a forensic approach to challenges.

#### PROFESSIONAL EXPERIENCE**:**

**Cybersecurity Analyst jun/8/2018 to Dec/1/2020**

**Sunrise Tech Solution**

Responsibilities for this position include:

* Constant monitoring of intrusion detection systems
* Creation of technically detailed reports based on intrusions and events
* Provides assistance in computer incident investigations
* Analyze and evaluate anomalous network and system activity
* Assist in troubleshooting and problem solving a wide variety of client issues
* Collaborate well with members of the IAM team on daily policy issues
* Provide quality customer service with excellent communication skills
* Recommend modifications to access control lists
* Provided internal security consulting for product development and operations of services across organization
* Worked with internal groups on their projects to help them achieve their goals
* Investigated, documented, and gathered information on data security recommendations to protect
* Led intrusion detection, vulnerability management, and PKI and participated in auditing incident
* Provided 24/7/365 systems support as necessary for the diverse needs of the organization

**Agile Scrum Master Jan 2017 to June 2018**

**Boston Security Firm**

* Facilitate sprint planning, daily scrums, retrospectives, stakeholder meetings, and
* software demonstrations
* Protect development team from outside distractions, impediments, or team conflicts, and maintain focus on product backlog project timeline
* Work closely with project owner in backlog management and continuous delivery of features
* Educate and reinforce scrum methodology and agile framework to team members and stakeholders
* Direct and lead development team from project initiation through the delivery of final product

**Project Manager / Scrum Master May 2010 to Jan 2016**

**PEEL, Inc.**

* Planned and monitored project spending/budgeting and guided projects to completion on time, within scope, and on budget
* Managed project scope to ensure delivery was compliant with scope commitment
* Tracked and managed product backlog, burn down metrics, velocity, and task breakdown
* Addressed problems through risk management and contingency planning

**Information Security Analyst 2009 to 2010**

**Bali Consulting Firm**

* Responsible to prepare review methods, analytical techniques, and compliance routines.
* Determine the internal control measures and ensure its strict implementation.
* Developed annual compliance training strategy and materials for the business units.
* Facilitated changes in the overall organizational policies to ensure alignment with the industry standards keep the business units updated with the changes in the applicable policies and standards
* Acted as a liaison between various departmental groups on information security related topic
* Audited systems based on security standards
* Collaborated in teams of technical and non-technical experts
* Conducted IT-Security standards/compliance assessments
* Developed detailed recommendations for mitigating findings and process improvement projects
* Developed mitigation strategies
* Documented results and presented findings to technical staff and management alike
* Drafted various policies and procedures
* Ensured compliance of Information Technology Security Policies and utilized vulnerability tools
* Fostered security-focused tools and training programs
* Identified and recommended solutions for various risks and security issues
* Maintained regulatory requirements
* Managed and facilitated information security related projects
* Moderated workshops and interviewed key stakeholders to determine technical threats and risk
* Monitored compliance with organization's information security policies and procedures
* Participated in tier 2/3 security operations support
* Planned security standards/compliance assessment projects based on a standardized offer and adapted to specific needs of our customers
* Presented and explained company's approach and methodology of security standards/compliance assessments and technical risk assessments to potential customers
* Provided expertise on IT-Security policies and guidelines, best practice approaches and solutions for compliance
* Validated and tracked security breach
* Worked with customers to determine their need for expert support in IT-Security, including applicability of standards, laws, and regulations to existing and future solution