



We make IT easy.™

From: Mike Onorato
DeVeera Inc.
5 Mandeville Ct.
Suite 100
Monterey, CA 93940

(831) 240-4703
mike@deveera.com

Prepared for: Suresh Prasad
Monterey Peninsula Water Management District
5 Harris CT
Building G
Monterey, CA 93940
United States
(831) 658-5600
suresh@mpwmd.net

Quantity	Description	Unit Price	Ext. Price
1.00	Network Security Assessment using CIS Protocol: Refer to Scope of Work Attachment	\$12,000.00	\$12,000.00
		Subtotal:	\$12,000.00
		Tax:	\$0.00
		Total:	\$12,000.00

Signature: _____

Date: _____

1 Introduction

1.1 Background

An information security assessment is a measurement of the security posture of a system or organization. The security posture is the way information security is implemented. Security assessments are risk-based assessments, due to their focus on vulnerabilities and impact. Security assessments rely on three main assessment methods that are inter-related. Combined, the three methods can accurately assess the Technology, People, and Process elements of security.

In the light of the recent ransomware attacks, Monterey Peninsula Water Management District has requested an evaluation of the security posture of the data and systems and processes that are currently being used by the organization in order to become more resilient to such attacks and prepare a better response such an event should occur.

1.2 Objectives

A security assessment is performed to identify the current security posture of an information system or organization. The assessment provides recommendations for improvement, which allows the organization to reach a security goal that mitigates risk, and also enables the organization.

The security assessment should enable one to answer the following questions:

- What is the critical information?
- What controls are in place for information systems?
- What is the current security posture of information systems?
- Should more or less stringent countermeasures be instituted?
- What is the prioritized security roadmap to follow that addresses high-priority issues first?

1.3 Scope of Work

Scope management is the process of defining what work is required, and then making sure that all of that work, and only that work, is done. The following processes will be covered in this project management knowledge area:

I. Collect Requirements

The Collect Requirements Process is critical. Unless requirements are understood & defined, it will be very difficult for the assessment to meet these requirements, and therefore the assessment will be far from a quality assessment.

- Requirements Related to The End Result of the Security Assessment
 - Requirements derived from customer expectations about assessment results, timeline, and cost.
 - Requirements to determine how well sensitive information is protected from disclosure, or to determine how well policy is achieving its purpose
 - Requirements to use one assessment method (reviewing, examination, or testing)
- Requirements Related to How the Work is Managed
 - Adherence to an established assessment methodology used by the organization.
 - Organization requirements with which assessments must comply.
 - Roles & responsibilities for both assessment team & target organization.
 - Assessment logistics, and assessors' skills & experience.
 - Data handling requirements (data storage, transmission, removal).

II. Define Scope

The Define Scope Process is primarily concerned with what is and is not included in the security assessment and its deliverables.

- Determine the assessment sites
- Define the size and number of systems and components to be assessed
- Details about the assessment method(s) to be used are defined

Using the CIS framework, a maximum number of 20 CSC controls can be evaluated depending on the Implementation Group agreed upon. The initial assessment will cover the first 6 CSC controls (e.g. Implementation Group 1 of the CIS framework):

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

The following aspects of every sub-controls will be evaluated as follows

1. whether or not the organization currently has a policy defined that indicates that they should be implementing the defined sub control
 2. whether or not the organization currently has implemented this sub control and to what degree the control has been implemented
 3. whether or not the organization currently has automated the implementation of this sub control and to what degree the control has been automated
 4. whether or not the organization is reporting this sub control to business representatives and to what degree the control has been reported
- Detailed rules of engagement are defined.
 - o specifying project progress reporting details
 - o how emergency communications will take place
 - o acceptable penetration testing times and whether they are announced or not
 - o details regarding the target organization observation of examination/testing activities performed
 - Deliverables
 - Level of Implementation for each CSC Control
 - Aggregate Scores representing the maturity levels for Policies, Controls
 - Levels of completion for each Implementation Group
 - The following ATT&CK activities will be assigned an overall score of *Low*, *Moderate*, or *High* for both *Preventive Capabilities* as well as *Detection Capabilities*
 - Initial Access
 - Execution
 - Persistence

- Privilege Escalation
 - Defense Evasion
 - Credential Access
 - Discovery
 - Lateral Movement
 - Collection
 - Command and Control
 - Exfiltration
- Project exclusions – to reduce likelihood of scope creep
 - Constraints & assumptions

III. Create Work-Breakdown-Structure (WBS) Process

A work breakdown structure is a very important tool. It increases project understanding, is deliverable-oriented, and divides the project into smaller manageable pieces. A WBS can also be used as a project communication tool. In the process of creating a WBS for a security assessment, we walk through the assessment and decompose deliverables into their smaller constituents, level by level. This is done until we reach a point where it is easy to estimate the cost, time, and resources to complete the lowest level of the structure. By completing a WBS for the security assessment, we help ensure that nothing in scope slips through the cracks, and nothing out of scope slips into the project.

IV. Verify Scope Process

The Verify Scope Process is the process of formalizing acceptance of the completed project deliverables. The deliverables are being reviewed and accepted by the customer, and not by the assessment team. The assessment team needs to first review and accept the completed deliverables before the customer reviews the deliverables for acceptance; however, the assessment team review activity is part of quality management and not scope management.

2 Tasks / Activities

The contractor shall provide proactive Risk and Vulnerability Assessment (RVA) capabilities which consists of several services available to test external and internal accessible systems, hosts, and applications in a stakeholder environment. There may be an overlap in requirements in some RVA services, however it is the specific methodology used to carry out the services in a RVA which make the services unique. The following tasks should be applied to each service:

TASK 1 – PRE ASSESSMENT PLANNING PHASE

During the pre-assessment phase, the assessment team and the organization being assessed must set expectations for each assessment and/or engagement.

SUBTASK 1.0 – Perform Initial Communication

The contractor shall work to schedule stakeholders according to their operating needs. The stakeholder organization should anticipate a two-week engagement period,

- one week being reserved for conducting interviews and evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities as well as review of documentation, architecture, rule-sets, and system configurations
- Another week required for hands-on technical process that looks specifically at the organization from a system/network level to identify security vulnerabilities that exist in those systems including technical analysis of the firewalls, intrusion detection systems, and routers. As well as vulnerability scans of the customer's networks

SUBTASK 1.1 - Deliver Rules of Engagement (ROE)

The purpose of the ROE is to establish the timeframe, scope and the activity that is allowed during an engagement and establish a binding agreement between the stakeholder and the contractor.

SUBTASK 1.2 - RVA Team/Stakeholder complete ROE

When the contractor receives a signed ROE from a stakeholder, it is countersigned and returned to the stakeholders to retain for their records.

SUBTASK 1.3 - Schedule RVA

Once the ROE is signed, returned, and verified, the RVA shall be scheduled and assigned a RVA Program Lead (contractor) who contacts the stakeholder with the testing dates, and communicates the default engagement timeline.

Week 1 – passive review techniques and interviews.

Week 2 – technical analysis of the active network devices: firewalls, intrusion detection systems, and routers. Vulnerability scans of the customer's networks.

The engagement timeline will be defined by organization for each assessment as the engagement may vary based on the scope of the engagement.

SUBTASK 1.4 – Conduct RVA Pre-Assessment Meeting

The RVA Program Lead (contractor) shall reach out to the designated stakeholder POC to schedule a Pre-Assessment Meeting to cover services, scoping, targets, expectations, and other logistics.

TASK 2 - TESTING/ASSESSMENT PHASE

During the assessment phase, the contractor is actively engaged in providing the selected service offerings to the stakeholder organization. The contractor Team Lead shall work closely to communicate current status with the designated stakeholder POC to ensure the engagement activity does not impact stakeholder business operations. Any major issues discovered during the assessment, including critical external vulnerabilities, shall be immediately communicated to the stakeholder organization. Stakeholder POC shall immediately be notified if suspected

classified information is found. If inappropriately stored PII is suspected, the team shall immediately seek clarification and next actions from the POC.

SUBTASK 2.0 - Commence RVA Engagement

At the beginning of the RVA Engagement, the contractor Team Lead shall provide the stakeholder with an in-brief that describes the action plan to deliver the RVA services. The Team Members shall provide support during the in-brief, answering specific technical questions and subject matter expertise as required.

Throughout the engagement, the contractor Team Lead shall provide written, and when requested, verbal, daily status updates with the designated POC.

SUBTASK 2.1 - Complete RVA Engagement

Once the selected services are completed and the systems are effectively assessed, the contractor Team Lead shall notify the designated stakeholder POC and schedule an out-brief presentation. The contractor Team Lead shall ensure all engagement data is provided to the POC, and a working copy is securely stored and retained for developing the final report as appropriate. All test systems shall be cleansed of stakeholder data prior to completion of the testing phase, except for a consolidated primary and backup working copy of the data for reporting purposes.

TASK 4 – POST ASSESSMENT PHASE

SUBTASK 3.0 - Reporting

The contractor RVA teams shall provide reports consistent with the organization requirements. Customization of the output is applied as needed. The report delivery process is as follows:

- The contractor Team Lead shall draft a report to the stakeholder two weeks after the completion of the RVA engagement.
- The Stakeholder shall review the draft report over the next one to two weeks.
- The contractor Team Lead shall deliver the final report after any modifications required based on the review of the draft report.

SUBTASK 3.1 - Mitigation Check

Six months after the final report is delivered the contractor RVA Program Lead or Team Lead shall send a notification to the stakeholder to review the status of any recommended mitigation action from the final report.

3 Business Terms / Conditions

3.1 Change Control/Change Order

Any changes in this statement of work will be documented in writing by (company name) Project Manager and submitted for written approval. Additional hardware, software, or services can be added to this project via Change Order and related Quote, which is to be approved prior to commencement of the additional project work.

EUGEN MATEI

5 MANDEVILLE CT #100 • MONTEREY, CA 93940
831 272 4340 • EUGEN@LEYLINECONSULTING.COM

SUMMARY OF QUALIFICATIONS

Senior level IT professional with in-depth knowledge and vast hands-on engineering experience in the areas of virtualization infrastructure, systems security, networking, storage, endpoint management in fast-paced customer oriented environments. Established reputation for exceptional people skills and ability to communicate at all levels of management, employees and vendors. Demonstrated leadership and reliability in critical situations. Summary of competencies includes:

- VMware infrastructure
- Microsoft Active Directory
- McAfee Endpoint Protection
- Network switching & routing
- Microsoft SCCM
- Systems security
- Storage
- Project management
- Protecting assets

PROFESSIONAL EXPERIENCE

LEILINE CONSULTING MONTEREY, CA
Cybersecurity Consulting

2019 – PRESENT

LEAD CYBER AND INFORMATION SECURITY ARCHITECT

Executed Security Risk Assessments and consulting services as they relate to CIS and NIST compliance and risk management, Data Security Architecture, and program development/maturity.

- ❑ Proficient with risk and security frameworks, standards, and best practices (e.g. HIPAA, COBIT, NIST, CSC, and ISO 27001/2)
- ❑ Assessed projects, changes, and new designs for appropriate audit points and intelligence gathering functionality.
- ❑ Performed Information Security Risk Assessments/Analyses.
- ❑ Performed Incident Monitoring and Analyses activities.
- ❑ Reviewed new and existing systems design projects and procurement plans for compliance with standards and architectural plans.
- ❑ Ability to think holistically and identify areas of technical and non-technical risk as well as mitigation or remediation options.
- ❑ Demonstrated experience with the NIST Cybersecurity Framework and auditing security controls identified in NIST SP800-171 and NIST SP800-53A;
- ❑ Strong knowledge of security standards and fundamentals such as OWASP Top 10, CVSS, CVE
- ❑ Security knowledge on current threats, trends, and mitigations
- ❑ Experience writing technical reports/presentations and presenting to non-technical audiences.

MONTAGE HEALTH MONTEREY, CA
Acute care regional hospital

2019 – PRESENT

VIRTUALIZATION ENGINEER

Responsible for supporting complex end-to-end network and VMware solutions in a Mission Critical environment. Hands on experience with communication protocols, Cisco UCS server architectures, networking technologies, network security solutions, and VMware Horizon View solution integration. Thorough understanding and analysis of systems and systems architecture of VMware VDI hardware and solution designs in order to provide guidance and support for optimization of VDI desktops.

- ❑ Monitoring virtualized systems on a regular basis to detect abnormal conditions.
- ❑ Escalating the problems to appropriate levels of IT management and/or vendor management when not resolved in a timely manner.
- ❑ Determining business needs by evaluating existing network infrastructure and systems.
- ❑ Ensuring that all assigned systems remain at vendor supported levels.

- ❑ Developing and documenting implementation plans for the installation/maintenance/upgrade of assigned systems.
- ❑ Developing and documenting test plans and thoroughly test system changes before and after implementation.
- ❑ Coordinating installation and maintenance of related software with other technical support personnel to assure maximum systems performance and minimum downtime.
- ❑ Installing security patches to assigned systems in a timely manner.
- ❑ Documenting all processes and procedures for any tasks performed on assigned systems.
- ❑ Owning issues and exceptions and work them through to resolution.
- ❑ Producing transparent written and verbal communications.
- ❑ Prioritizing time and financial spend to maximize spend / risk reduction return.
- ❑ Ensuring expectations for delivery or resolution are met and communicated transparently to all parties, both internal and external.

SALINAS VALLEY MEMORIAL HEALTHCARE SYSTEM SALINAS, CA

2004 – 2019

Acute care regional hospital

SYSTEMS SECURITY ARCHITECT

2017 – 2019

Responsible for the majority of IT security functions, ranging from preventive security controls to activity monitoring and threat/behavior detection mechanisms. Ensuring the privacy, integrity and availability of sensitive data both at rest and in motion. Understanding business mission and aligning the security program with the strategic, operational and tactical goals of the business, in order to facilitate future growth and adoption of new technology.

- ❑ Implement, maintain, and monitor Imprivata OneSign single sign-on solution, and integrating it with VMware Horizon View VDI instant clone technology on Windows 10 Enterprise platform
- ❑ Manage and maintain VMware Horizon View VDI infrastructure to facilitate medical personnel access to critical EMR applications internally as well as externally
- ❑ Build and maintain multiple virtual desktop environments using VMware Horizon View instant clone technology, RDSH, linked clones and persistent disks
- ❑ Manage on premise enterprise virtualization environment using vSphere and vRealize
- ❑ Build and configure layer 2 and layer 3 networks, integrating Cisco networking equipment and VMware virtual distributed switch technology
- ❑ Build, configure and operate on premise Microsoft's System Center Configuration Manager, facilitating the management of Active Directory Windows endpoint systems including patch management, software deployment, hardware and software inventory, zero touch operating system deployment, and security baselining
- ❑ Manage and maintain enterprise antivirus endpoint systems using McAfee ePolicy Orchestrator
- ❑ Manage and maintain on premise enterprise email filtering cluster system provided by Proofpoint, including secure messaging
- ❑ Manage and maintain enterprise internal and external PKI certificate authorities
- ❑ Maintain, monitor, and upgrade enterprise Active Directory domain controllers and DNS service
- ❑ Conduct day-to-day operation, monitoring and maintenance of enterprise internal, perimeter and branch offices Checkpoint firewall clusters and standalone appliances.
- ❑ Install, operate and monitor JunosPulse Connect Secure appliance cluster
- ❑ Implement and enforce information systems security policies
- ❑ Maintain System Security Plans and all other system security documentation, reviewing and updating them at least annually, for all assigned systems.
- ❑ Ensure the implementation and maintenance of security controls in line with the Security Program
- ❑ Manage and control changes to the security systems, and conduct assessments on potential security implications/outcomes
- ❑ Ensure that system security requirements are addressed during all phases of the IS lifecycle
- ❑ Configure, maintain, and monitor two-factor authentication solution (Duo)
- ❑ Implement a strategy for continuous monitoring of assigned systems including: establishing system audit trails and ensuring their review; reporting all identified security findings; and initiating the periodic review of security controls

- ❑ Ensure security awareness and precautionary measures are exercised to prevent introduction and/or proliferation of malicious code or other adverse IS conditions
- ❑ Advise the System Owners regarding security considerations on various applications
- ❑ Serve as a resource for users concerning all security questions regarding assigned systems and applications
- ❑ Conduct technical evaluation of information system design, focusing on information security aspects and accreditation
- ❑ Use various information system inspection tools, to audit systems, analyze potential vulnerabilities, and identify mitigation approaches
- ❑ Perform vulnerability/risk assessment analysis to support accreditation and other program protection activities
- ❑ Coordinate with third-party vendors to find vulnerabilities and improve the overall security posture
- ❑ Review requests for software installation and conduct technical risk assessment on software implementation
- ❑ Conduct validating and deploying tasks associated with Windows OS patches and various applications patches on a regular basis
- ❑ Coordinate and track security action requests and status
- ❑ Conduct periodic assessments of systems, to ensure compliance with security requirements using NIST 800-53 framework in accordance with HIPAA rule

IT SECURITY ANALYST

2008 – 2017

- ❑ Installed, configured and centrally managed multiple branch office firewall systems facilitating access to locally hosted web ambulatory EMR system
- ❑ Responsible for installing, configuring, and maintaining extranet access systems
- ❑ Monitored uptime and resource availability of critical infrastructure equipment
- ❑ Maintained data and monitored security access
- ❑ Analyzed IT requirements and provided objective advice on the use of IT security systems
- ❑ Tested and evaluated new technologies
- ❑ Designed, analyzed and implemented efficient IT security systems
- ❑ Planned, implemented and upgraded security measures and controls
- ❑ Established plans and protocols to protect digital files and information systems against unauthorized access, modification and destruction
- ❑ Anticipated and alerted hardware and software failures based on logging analysis
- ❑ Managed and maintained network intrusion detection and prevention systems
- ❑ Recommended and installed appropriate tools and countermeasures to improve overall security posture
- ❑ Coordinated and facilitated the transmission of PII data in a secure manner to and from outside vendors and other entities.
- ❑ Created procedures to audit and alert on data changes such as updates, deletion or moving
- ❑ Reviewed organization's firewall policy periodically to ensure compliance with the security program as well as to improve system reliability, availability, serviceability, and performance.

NETWORK ENGINEER

2007 – 2008

- ❑ Provided technical support for Network Servers and software configuration for all medical and business related systems.
- ❑ Responsible for the implementation and maintenance of the vertical (single and multi-mode fiber) and horizontal (Cat 3 to Cat 6) infrastructure for both voice and data communications.
- ❑ Implemented, monitored and supported LAN and WAN with an emphasis on layers one through four of the OSI protocol stack.
- ❑ Managed change control process, documentation, TCP/IP addresses, developed and maintained topology maps and network diagrams, used in debugging and quick identification of issues.
- ❑ Developed, configured and implemented equipment of the converged technology infrastructure (voice/data).

IT SYSTEMS ADMINISTRATOR

2006 – 2007

- ❑ Monitored & maintained Microsoft SMS platform health and mitigate identified problems

- ❑ Implemented Systems Management Server to assist with mass deployment mechanisms of software patches and upgrades in Windows environment.
- ❑ Created automated software deployments and operating system zero-touch in-place installation
- ❑ Planned, tested, managed and implemented upgrades to new versions of software & hardware on endpoint desktop systems
- ❑ Performed root cause analysis & troubleshooting support of installation and deployment issues with various IT and business groups.
- ❑ Responsible for yearly true up of organization's Microsoft Volume Licensing program

IT SYSTEMS TECHNICIAN

2004 – 2006

- ❑ Responsible for the maintenance, configuration, and reliable operation of desktop computer systems throughout the organization
- ❑ Researched and diagnosed hardware and software errors by running diagnostics, documenting problems and resolutions, prioritizing, and assessing impact of issues
- ❑ Followed standard procedures for proper escalation of unresolved issues to the appropriate internal teams
- ❑ Installed and upgraded computer components and software
- ❑ Interacted with vendors, outsourcers, and contractors
- ❑ Created and revised technical documentation
- ❑ Participated in standard Windows image development, management, QA testing, and deployment

MONTEREY PENINSULA COLLEGE MONTEREY, CA

2003 – 2008

Education

IT TECHNOLOGIST

Responsible for the operational aspect of two computer labs (Windows and Apple OS) including application deployments, performance improvements, operating system upgrades and patches.

- ❑ Developed and implemented the use of Microsoft RIS service to assist with systems recovery from failure as well as deployment of new systems
- ❑ Built and deployed windows images using RIS server and PXE network boot
- ❑ Troubleshoot installed applications and helped when needed during classes
- ❑ Managed student accounts and respective file shares

E D U C A T I O N

BS, Physics • *University of Bucharest* • Romania

T E C H N I C A L C E R T I F I C A T I O N S

MCSE • CISSP • VCAP-DTM • VCP-DCVNV • VCP-DTMNV

International Information System Security Certification Consortium

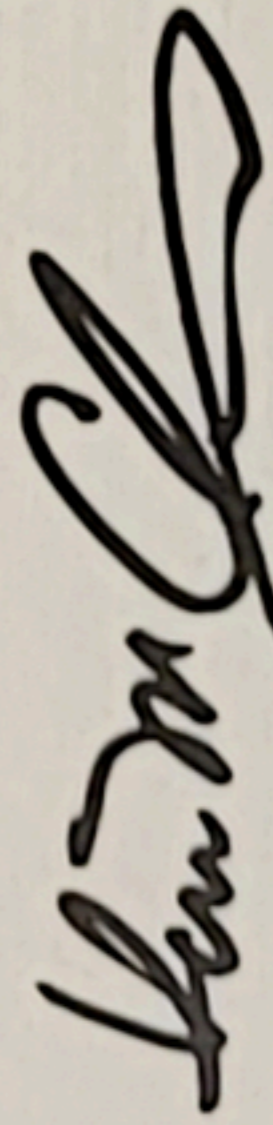
The (ISC)² Board of Directors hereby awards

Eugen Mlatei

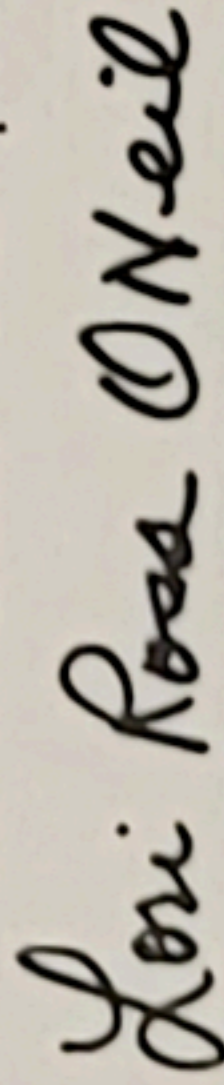
the credential of

Certified Information Systems Security Professional[®]

having met all of the certification requirements, which include the professional experience prerequisite, adoption of the (ISC)² Code of Ethics, and successful performance on the required competency examination, subject to recertification every three years, this individual is entitled to all of the rights and privileges associated with this designation, as defined in the (ISC)² Bylaws.



Dr. Kevin Charest - Chairperson



Lori Ross O'Neil - Secretary



ID# 813271

Certification Number

Aug 1, 2020 - Jul 31, 2023

Certification Cycle

Certified Since 2020