### Position Description

<table>
<thead>
<tr>
<th>Position Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report Run Date</strong></td>
</tr>
<tr>
<td><strong>Position Number:</strong></td>
</tr>
<tr>
<td><strong>Dept:</strong></td>
</tr>
<tr>
<td><strong>Position:</strong></td>
</tr>
<tr>
<td><strong>Approved Payroll Title Code:</strong></td>
</tr>
<tr>
<td><strong>Approved Payroll Title:</strong></td>
</tr>
<tr>
<td><strong>Approved MSP Salary Grade:</strong></td>
</tr>
<tr>
<td><strong>Approved PSS Salary Grade:</strong></td>
</tr>
</tbody>
</table>

#### POSITION DETAILS

<table>
<thead>
<tr>
<th>Job Summary:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under the general direction of the Deputy Chief Information Security Officer (DCISO), manages security and data protection solutions that support the mission of the university and protect the confidentiality, integrity, and availability of information assets owned or entrusted to UC Davis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Campus Job Scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new and existing information technology (IT) systems meet the University's information assurance (IA) and security requirements. Prepares/maintains various security reports and dashboards, participates in technology audit activities, prepares and reviews system security architecture designs, actively participates with business and campus units throughout the university community,</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department Specific Job Scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracks and reports on security risks and control effectiveness to the CISO and other campus stakeholders such as the Chief Information Officer, Network Operations Managers, security professionals located at the Davis and Sacramento campuses and other campus IT leaders.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department Specific Job Scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stay abreast of evolving campus needs, technology capabilities, and threat intelligence from a variety of sources to optimize data protection measures. Works with campus stakeholders to ensure data security needs and controls are aligned to support organizational goals and objectives and uses independent thinking to creatively solve problems and issues, makes independent decisions, and must maintain or preserve confidentiality when required to do so.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department Specific Job Scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Information Security Analyst will create a positive environment where the other members of the security team can enhance their skills as security professionals.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Department Specific Job Scope:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The functions that the risk assessor manages are critical to the mission of the University, requiring the system assessor to be available 24x7.</td>
</tr>
</tbody>
</table>
Positions Supervised: N/A

Essential Responsibilities:

20% INFORMATION SECURITY CONSULTING
- Provide information security subject matter expert consulting.
- Perform information security analysis & assessments on new systems, network devices, and applications with recommendations & assessment results provided to stakeholders.
- Prepare new, and maintain existing, security assessment checklists and analysis documentation as required to ensure security assessments are reliable, efficient, and effective.
- Provide formal assessment reports to management including mitigation recommendations & status.

65% RISK ASSESSMENT
- Develop methods to monitor and measure risk, compliance, and assurance efforts.
- Consult with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
- Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.
- Integrate and align information security and/or information assurance (IA) policies to ensure system analysis meets security requirements.
- Develop an enterprise system security context, a preliminary system security concept of operations, and define baseline system security requirements in accordance with applicable information assurance (IA) requirements.
- Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.
- Draft statements of preliminary or residual security risks for system operation.
- Maintain information systems assurance and accreditation materials.
- Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.
- Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks.
- Plan and conduct security authorization reviews and assurance case development for initial installation of software applications, systems, and networks.
- Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant information assurance (IA) compliances.
- Recommend new or revised security, resilience, and dependability measures based on the results of reviews.
- Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
- Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
- Verify that the software application/network/system accreditation and assurance documentation is current.
- Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).
- Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system.

15% DOCUMENTATION & GOVERNANCE
- Prepare, maintain, and review various security standards, guidelines, and policies.
- Prepare/maintain measurement documentation including reports, dashboards, & other security related metrics or documents.
Develop/assist with the creation of formal request and procurement related documents such as RFPs, RFQs, Purchase Requests, and Response Scoring. Participate in research of IT security tools, techniques, methodologies, technologies, and architectures. Participate on various security & technology related committees and workgroups.

**Physical Demands:**

- Work alternate or extended hours on short notice.
- Occasional travel is required to campus and off campus worksites.
- Due to the mission-critical services provided by this department, this position may work hours other than M-F 8-5, especially during system development, hardware or software installation, or in response to system problems.

UC Davis is a smoke and tobacco free campus effective January 1, 2014. Smoking, the use of smokeless tobacco products, and the use of unregulated nicotine products (e-cigarettes) will be strictly prohibited on any UC Davis owned or leased property, indoors and outdoors, including parking lots and residential space.

**Background Check:**

Yes

**QUALIFICATIONS**

**Minimum Qualifications:**

- Experience to use Risk Management Framework (RMF) requirements.
- Experience using information security frameworks and standards such as ISO, NIST and regulations related to information security such as PCI, HIPAA, FISMA, SB 1386, etc.,
- Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities.
- Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.
- Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation.
- Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures.
- Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities.
- Skills to organize and manage time to meet all task and project goals and to provide project reports as requested by clients and management Experience to coordinate several simultaneous activities with strict deadlines, complex scheduling requirements, and little or no tolerance for errors or delays.
- Strong proficiency with common productivity software such as Microsoft Visio and Excel.

**Preferred Qualifications for Selection:**

- Bachelor's degree in related area and/or equivalent experience/training.
- Intermediate experience as an information security professional.
- CRISC, CISSP, CISA, GIAC or PCI certifications.
- Knowledge of the organization's core business/mission processes.
- Knowledge of the organization's enterprise information technology (IT) goals and objectives University experience preferred.
- CISSP, CISM, CISA or GIAC certifications.
- Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth).
- Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.

**Expectations**

- Read and model the UC Davis Principles of Community
- Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.
- Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation.
- Knowledge of information technology (IT) supply chain security/risk management policies, requirements, and procedures.
- Adhere to workplace safety practices, read information communicated about workplace safety, complete required safety training on time, report any workplace safety issues promptly to their supervisor or the designated safety coordinator.
- Communication skills to effectively present information (oral, written, presentation, documentation).
- Use tact and diplomacy for interactions with others.
- Communication skills to understandably and effectively describe technical requirements to technical and non-technical audiences.
- Provide higher level technical assistance to the technical workforce in the resolution of abnormal operating conditions.
- Support departmental goal of providing positive, innovative and effective customer service through performance of job functions.
- Work cooperatively with others to achieve and maintain a strong client service environment.
- Highly motivated and results orientated.
- Maintain flexibility in a continuously changing and fast paced work environment.
- Excellent organizational and analytical skills.
- Ability to work independently under general direction from management, to manage workload across multiple simultaneous projects, to maintain a high level of productivity, and to meet deadlines under time constraints and continuously shifting priorities.
- Maintain up-to-date knowledge through literature, classes, exhibits, seminars, on-the-job training and other relevant training forums.
- Willingness to learn and apply new technology and willingness to promote professional growth.
- Willingness to routinely stay in communication with technical staff at other organizations to stay abreast of computing developments and resources available over the network.
- Accountability for the safekeeping of resources in the employee's care and custody and for following and implementing the cyber-safety guidelines.
- Work cooperatively and collaboratively with others in support of the mission of UCD.
- Demonstrate flexibility and willingness to assist in other areas of the department when needed.
- Ability to cultivate trust and build successful working relationships with stakeholders, subject matter experts, and other relevant staff and management.
- Work with a diverse group of people in such a manner as to build high morale and group commitments to goals and objectives.