|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| State of California  California department of technology **Proposed**  Duty Statement  Tech 052 (Rev. 02/2018) | | | | | | **RPA NUMBER (HR Use Only)** | | | |
| 23-034 | | | |
| **ALERT: This form is mandatory for all Requests for Personnel Action (RPA).**  **INSTRUCTIONS:** Before completing this form, read the instructions located on last page. | | | | | | | | | |
| Section A: Position Profile | | | | | | | | | |
| A. Date | | B. appointment effective date | | C. Incumbent Name | | | | | |
| September 26, 2023 | |  | |  | | | | | |
| d. CIVIL SERVICE CLASSIFICATION | | | | e. POSITION WORKING TITLE | | | | | |
| Information Technology Manager I | | | | Information Technology Auditor | | | | | |
| F. Current Position Number | | | | G. proposed Position Number (Last three (3) digits assigned by HR) | | | | | |
| 695-405-1405-003 | | | |  | | | | | |
| H. office / section / unit / physical Location of Position | | | | I. supervisor Name and classification | | | | | |
| Office of Information Security/Audit Program, Rancho Cordova | | | | Michael Stanford, Information Technology Manager II | | | | | |
| J. Work Days / Work Hours / work shift (day, swing, grave) | | | | K. Position Requires: | fingerprint background check | | | | Yes  No |
| Monday-Friday 8:00 a.m. to 5:00 P.M. | | | | Driving an Automobile | | | | Yes  No |
| Section B: Position Functions and Duties  **Identify the major functions and associated duties, and the percentage of time spent annually on each (list higher percentages first).** | | | | | | | | | |
|  | **Information Technology Domains (Select all domains applicable to the incumbent’s duties/tasks.)** | | | | | | | | |
| Business Technology Management  Information Security Engineering | | | IT Project Management  Software Engineering | | | Client Services  System Engineering | | |
|  | Organizational Setting and Major Functions  Under the general direction of the Information Technology Manager II, (ITM II) the Information Technology Manager I (ITM I) will serve as an Information Systems Security Auditor and part of a statewide Information Security Audit Program team. The incumbent is responsible for timely execution of high quality information system security audits of state agency technology infrastructure and information security programs, business application systems, and significant projects to validate requisite information security controls are in place and are working as intended. | | | | | | | | |
|  |  | | | | | | | | |
| %of time performing duties  50%  45% | Essential Functions (Percentages shall be in increments of 5, and should be no less than 5%.)  Plan, conduct and manage information security program audits. Specific duties include:   * Plan, schedule and perform preliminary analysis for assigned audit projects. * Identify, plan and communicate audit scope, objectives, approach, timing and deliverables with affected parties. * Identify, document and map technology processes and internal controls in accordance with scope of the audit projects. * Complete audit testing including inquiry, observation, and other analysis to verify Compliance with the security objectives. * Prepare and maintain accurate working papers which support sound audit conclusions.   Prepare and maintain audit time records and monitor performance against approved schedule and budget.   * Communicate progress and results of audit throughout the audit engagement to audited agencies and management. * Develop recommendations to address security objectives and other areas of concern identified during assigned audits. * Prepare audit reports and formally present and communicate audit results and related recommendations. * Monitor implementation of controls related to outstanding audit findings and validate their implementation. * Ensure the audit manual is kept up to date by making the necessary edits that capture the auditor processes and procedures for each step in the audit workflow. | | | | | | | | |
|  |  | | | | | | | | |
|  | Marginal Functions (Percentages shall be in increments of 5, and should be no more than 5%.) | | | | | | | | |
| %of time performing duties  5% | * Assist with other statewide program representation, training and related activities * Conduct training and make presentations on audit requirements; * Participate and provide input into federal, state and multi-jurisdictional committees, working group products and services, such as the Multi-State Information Sharing and Analysis Center work groups that benefit the U.S government sector; * Prepare executive management reports of findings, including identification of statewide problems, trends, and recommendations and alternatives to mitigate risk. * Other related duties. | | | | | | | | |
|  | Work Environment Requirements  Work is conducted in a professional office environment. Business dress, according to current office policy, is required. This position requires the ability to work excess hours, to effectively work under pressure to meet deadlines, use of a computer to communicate and prepare written materials, and the ability to travel to meetings, audit locations and conferences at various locations. The position will report to various department locations during audit execution. | | | | | | | | |
|  | **May be eligible for telework and when permitted incumbent is:**   * Required to support a work from home environment. * Expected to maintain a secure workspace within their home and support necessary logistical requirements to support remote video conferencing and remote work. Maintain a secure work from home environment for all work materials to ensure they are not misused, lost, damaged, stolen or improperly disclosed. | | | | | | | | |
|  | Allocation Factors (Complete each of the following factors.) | | | | | | | | |
|  | **Supervision Received:**  The Information Technology Manager I receives general direction and supervision from the Information Technology Manager II.    **Actions and Consequences:**  The incumbent is responsible for the planning, design and execution of information security audits of state agency department’s highly complex information systems and programs. The incumbent is required to have knowledge of Government Accountability Office's Generally Accepted Government Auditing Standards, and the American Institute of Certified Public Accountant's Statements on Auditing Standards, and Information Systems Security Audit and Assurance Standards. This program has significant statewide impact and is part of the overall state information security program. The consequences of error (lack of adherence to audit standards and accuracy) results in increased security risk exposure and liability for the state.    **Personal Contacts:**  This position will interact with all levels of staff including state agency and departmental Agency Directors, Agency Information Officers, Chief Information Officers, Information Security Officers, Privacy and Disaster Recovery Coordinators, and stakeholders from other branches and levels of government, education, critical infrastructure sectors, National Associations, and private industry.    **Administrative and Supervisory Responsibilities: (Indicate “None” if this is a non-supervisory position.)**  This position manages all aspects of the assigned audits.  **Supervision Exercised:**  The position will serve as a project and program leader over department audit projects and initiatives with significant statewide impact. The position will lead and direct audited agency staff in the execution of audit functions. | | | | | | | | |
|  | Other Information | | | | | | | | |
|  |  | | | | | | | | |
|  | **Desirable Qualifications: (List in order of importance.)**   * Experience performing audits in the field of information technology are preferred. * A Bachelor's degree in Science, Business and/or Security; Master's Degree in Business Administration and/or degree in Technology are preferred * It is highly preferred that the incumbent possess and maintain one or more of the following professional security industry recognized certifications: The Certified Information Systems Auditor (CISA) certification is preferred; other certifications in information security or auditing such as Certified Internal Auditor (CIA),Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC) or Certified Information Systems Security Professional (CISSP) other audit certifications are also desirable. * Extensive knowledge of federal and state information security policies, standards, principles, practices and frameworks. (SAM 5300 - NIST 800-53). * Excellent verbal and written communication skills. * Ability to effectively present information clearly to staff and auditees at all levels and at a wide variety of state entities to prepare entities for audit activities. * Some travel required for meetings, trainings and conferences. * Ability to prepare detailed audit reports, presentations and other types of audit related documentation on short notice. * Ability to develop and maintain effective and cooperative working relationships. * Possess mature interpersonal skills and will be a supportive team member. * Business casual dress code at entity sites are required. (Monday-Friday). * Ability to work in a fast pace and changing environment and is able to adopt and support change as needed. We are looking for a team-oriented candidate. | | | | | | | | |
|  |  | | | | | | | | |
| **incumbent Statement: I have discussed the duties of this position with my supervisor and have received a copy of the duty statement.** | | | | | | | | | |
| Incumbent Name (Print) | | | Incumbent Signature | | | | | Date | |
|  | | |  | | | | |  | |
| **Supervisor Statement: I have discussed the duties of this position with the incumbent.** | | | | | | | | | |
| Supervisor Name (Print) | | | Supervisor Signature | | | | | Date | |
| Michael Stanford | | |  | | | | |  | |