



## Manager, Security Risk and Third Party Management Job Description

### JOB INFORMATION

|                          |   |
|--------------------------|---|
| <i>Job Code:</i>         | 166099  |
| <i>Job Title:</i>        | Manager, Security Risk and Third Party Management       |
| <i>FLSA Status:</i>      | Exempt  |
| <i>Supervisory:</i>      | May oversee student, temporary and/or resource workers. |
| <i>Job Family:</i>       | IT Security   |
| <i>Job Family Group:</i> | Information Technology                                  |
| <i>Management Level:</i> | 5 Manager   |

### JOB SUMMARY

Oversees risk assessments, defines risk management and standard security contractual requirements, and partners with risk owners to mitigate third-party security risks. Maintains a process for assigning risk ratings, manages an inventory of third-party vendors, and oversees incorporation of standard security requirements into their contracts. Communicates security objectives, initiatives, threats and risks to all schools, units and hospitals, and provides them guidance in developing and implementing risk treatment plans.

### JOB QUALIFICATIONS:

#### Education

| <i>Req</i> | <i>Pref</i> | <i>Degree</i>     | <i>Field of Study</i> |
|------------|-------------|-------------------|-----------------------|
| X          |             | Bachelor's degree |                       |
|            | X           | Master's degree   |                       |

#### Additional Education

**Check here if experience may substitute for some of the above education.**

Combined experience/education as substitute for minimum education

#### Work Experience

| <i>Req</i> | <i>Pref</i> | <i>Work Experience</i> | <i>Experience Level</i> |
|------------|-------------|------------------------|-------------------------|
| X          |             | 7 years                |                         |
|            | X           | 10 years               |                         |

#### Additional Work Experience

**Check here if education may substitute for some of the above work experience.**

Combined experience/education as substitute for minimum work experience

#### Knowledge, Skills and Abilities

| <i>Req</i> | <i>Pref</i> | <i>Functional Skills</i>   |
|------------|-------------|--|
| X          |             | Strong understanding of regulatory requirements (e.g., GLBA, PCI, FERPA, HIPAA) with subject matter-expert knowledge in one or more areas. |
| X          |             | Broad breadth of technical skills and experience in IT, security and privacy.  |

## Knowledge, Skills and Abilities

| <i>Req</i> | <i>Pref</i> | <i>Functional Skills</i>   |
|------------|-------------|--|
| X          |             | Strong understanding of information security across all security domains, and the relationship between threats, vulnerabilities and information value in the context of risk management.               |
| X          |             | Significant experience in risk management, audit, assessment and/or internal controls.   |
| X          |             | Experience with legal and regulatory requirements and industry security frameworks.  |
| X          |             | Experience performing information security risk assessments and risk analysis.   |
| X          |             | Demonstrates an understanding of processes, internal control risk management, information security controls, and how they interact together.   |
| X          |             | Communicates and presents security risk concisely and effectively in relation to enterprise risk based on the appropriate level of management and stakeholder groups.                                  |
| X          |             | Strong understanding of contractual agreement management and writing skills.   |
| X          |             | Experience performing information security risk assessments and risk analysis.   |
| X          |             | Demonstrates leadership and problem-solving skills.  |
| X          |             | Possesses advanced interview skills to tailor the types of questions based on responses provided by internal personnel or third parties.   |
| X          |             | Communicates and presents security risk concisely and effectively in relation to enterprise risk based on the appropriate level of management and stakeholder groups.                                  |
|            | X           | Strong understanding of applicable and accepted audit and risk frameworks (e.g., COBIT, NIST, ISO) and government guidelines and laws (e.g., FERPA, HIPAA).  |
|            | X           | Demonstrable progressive roles in career.  |
|            | X           | Experienced in presenting to large groups with confidence and polished presentation skills.  |
|            | X           | Experience with GRC and Vendor Risk Management tools.  |
|            | X           | Competency in customer focus, change and innovation, strategic thinking, relationship thinking, relationship building and influencing, talent management, results focus, and inspirational leadership. |
|            | X           | Ability to manage effectively and work closely with business leaders in a high pressure, fast paced, highly collaborative environment with multiple deadlines and competing priorities.                |

## Certifications

| <i>Req</i> | <i>Pref</i> | <i>Select Certifications</i> | <i>Enter Additional Certifications</i>             |
|------------|-------------|------------------------------|--|
|            | X           |                              | Working toward or has CISA or CISSP certification. |

## Other Job Factors

## JOB ACCOUNTABILITIES

|  | <i>% Time</i> | <i>Essential</i> | <i>Marginal</i> | <i>N/A</i> |
|--|---------------|------------------|-----------------|------------|
| Oversees monitoring and analyzing of all risks associated with third parties in scope, and determines overall risk profile and health of the third parties. Manages information security risk assessments in alignment with the information security strategy. |               |                  |                 |            |
| Manages consultation on current business processes to redesign for risk reduction, best practice compliance with regulatory requirements, efficiency and effectiveness.  |               |                  |                 |            |
| Monitors and measures effectiveness of risk treatment activities through the security metrics and risk remediation programs.   |               |                  |                 |            |
| Works with and manages partnerships with legal, procurement and related groups to define the standard security contractual requirements and develop service-specific language as required to facilitate, mitigate, and identify third-party security risks.    |               |                  |                 |            |
| Provides guidance to Schools, Units and Hospitals in development and implementation of risk treatment plans based on established risk-level, service-level agreements (SLAs), or on risk acceptance based on approved acceptance criteria.                     |               |                  |                 |            |
| Defines third party secure management requirements, security assessment process and assessment triggers for management of third parties across the third-party   |               |                  |                 |            |

## JOB ACCOUNTABILITIES

|  | <i>% Time</i> | <i>Essential</i> | <i>Marginal</i> | <i>N/A</i> |
|--|---------------|------------------|-----------------|------------|
| management lifecycle (on-boarding, on-going assessment, and service or contract termination).  |               |                  |                 |            |
| Maintains process for assigning risk ratings to new third parties and vendors, and confirms that new third parties and vendors are assigned a risk rating.   |               |                  |                 |            |
| Contributes to the enhancement in tools and methodologies used to assess risk; establishes guidelines and tools to facilitate continuous improvement in related initiatives by performing business risk analysis and providing leadership to internal business partners.   |               |                  |                 |            |
| Oversees engagements with project teams to strengthen the operational risk posture of the organization, and establishes appropriate operational risk and security standards.   |               |                  |                 |            |
| Recruits, screens, hires, trains and directly supervises all assigned subordinate staff. Evaluates employee performance and provides guidance and feedback. Counsels, disciplines and/or terminates employees, as required. Recommends departmental goals and objectives, including workforce planning and compensation recommendations. Reassesses or redefines priorities as appropriate in order to achieve performance objectives.   |               |                  |                 |            |
| Maintains awareness and knowledge of current changes within legal, regulatory, and technology environments which may affect operations. Ensures senior management and staff are informed of any changes and updates in a timely manner. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations and publications. Attends meetings, seminars and conferences and maintains continuity of any required or desirable certifications, if applicable. |               |                  |                 |            |

## Other Requirements

| <i>Essential:</i>  | <i>Emergency Response/Recovery</i>   | <i>Essential:</i> | <i>Mandated Reporter</i>  |
|--|--|-------------------|---|
|  | In the event of an emergency, the employee holding this position is required to “report to duty” in accordance with the university’s Emergency Operations Plan and/or the employee’s department’s emergency response and/or recovery plans. Familiarity with those plans and regular training to implement those plans is required. During or immediately following an emergency, the employee will be notified to assist in the emergency response efforts, and mobilize other staff members if needed. |                   | A mandated reporter who in his or her professional capacity has knowledge of, or reasonably suspects a person who is under the age of 18 years, elderly, or a dependent adult has been the victim of abuse or neglect must report the suspected incident. The reporter must contact a designated agency immediately or as soon as practically possible by telephone or in writing within 36 hours. By virtue of the associated job duties, this position qualifies as a mandated reporter as required by state law and USC’s policy at: <a href="https://policy.usc.edu/mandated-reporters/">https://policy.usc.edu/mandated-reporters/</a> |
| <i>Campus Security Authority (CSA)</i>   |  |                   | <i>Essential:</i>   |
| By virtue of the associated job duties, this position qualifies as a Campus Security Authority as required by law and USC’s policy at: <a href="https://dps.usc.edu/alerts/clery/">https://dps.usc.edu/alerts/clery/</a> |  |                   | No  |

## ACKNOWLEDGMENTS

The above statements reflect the essential and non-essential functions as necessary to describe the principle contents of the job. They are not intended to be a complete statement of all work requirements or duties that may be required of the position. I understand that I may be asked to perform other duties as assigned. USC reserves the right to add or change duties at any time.

The University of Southern California is an Equal Opportunity Employer. USC prohibits discrimination on any basis protected under federal, state, or local law, regulation, or ordinance or university policies. All employment decisions are based on individual qualifications and business need.

I acknowledge receipt of this job description and its associated physical requirements. I have read and understand the job description and job requirements and agree to abide by their contents. I realize that duties may be requested of me that are not specifically stated herein. I understand that I will be expected to adjust to potential fluctuations in work volume. I understand that, if I have any questions about the essential functions or expectations of my position, my supervisor and/or HR partner are available to discuss them with me.

\_\_\_\_\_  
Print Employee Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Manager Name

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

This job description describes the general nature and level of work required by the position. It is not intended to be an all-inclusive list of qualifications, skills, duties, responsibilities or working conditions of the job. The job description is subject to change with or without notice, and Management reserves the right to add, modify or remove any qualification or duty. Nothing in this job description changes the existing at-will employment relationship between the university and the employee occupying the position.