



JOB INFORMATION

Job Code:	166095
Job Title:	Lead, Third Party Management
FLSA Status:	Exempt
Supervisory:	May oversee student and/or temporary workers.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	5 Manager

JOB SUMMARY

Monitors and analyzes all risks associated with third parties, determines their overall risk profile and health, and maintains inventory of vendors assessed. Partners with business and risk owners on third-party exits and project plans, reviews and executes secure management requirements, assessment processes and assessment triggers for the entire management lifecycle, and maintains an inventory of all vendors assessed. Implements process for and confirms assignment of risk ratings to new third parties and vendors, incorporates standard security requirements in contracts, and obtains legal and security guidance on changes. Performs risk assessments, promotes oversight and governance across business operational areas throughout the university, and develops, documents and maintains enterprise-wide policies across the university.

JOB QUALIFICATIONS:

Education

Req	Pref	Degree	Field of Study
X		Bachelor's degree	
	X	Master's degree	

Additional Education

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

X Combined experience/education as substitute for minimum education

Work Experience

Req	Pref	Work Experience	Experience Level
X		5 years	
	X	5 years	

Additional Work Experience

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

X Combined experience/education as substitute for minimum work experience

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Strong understanding of the principles of risk management, information security, and their relationship to corporate governance activities such as operational risk assessment and organizational impact.

Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		In-depth knowledge of industry standards of risk analysis approaches (e.g., ISO, COBIT, COSO), as well as regulatory standards (e.g., SOX, FERPA, GLBA, HIPPA), and business resiliency approaches.
X		Strong understanding of compliance, fraud and risk mitigation methodologies to enhance business operational efficiencies.
X		Highly developed, effective oral and written communication skills that are utilized to inform, inspire and influence others in a clear and concise manner.
	X	Proven ability to balance multiple priorities, adapt to a constantly changing business environment, work independently, drive projects to completion, and meet deadlines in a fast-paced environment with only periodic supervision.
	X	Ability to work collaboratively and manage and initiate effective cross-functional relationships maintaining a high level of professionalism, self-motivation, and a strong sense of urgency.
	X	Strong computer skills, including MS Office products (e.g., Word, Excel, PowerPoint, Visio) and other business software to prepare reports, memos, summaries and analysis.
	X	Experience with GRC and Vendor Risk Management tools are a plus.
	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.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Monitoring and analyzing all risks associated with third parties in scope, and determining overall risk profile and health of the third parties.				
Partnering with business and risk owners on third party exits and associated project plans.				
Reviews and executes third party secure management requirements, security assessment process, and assessment triggers for management of third parties across the third party management lifecycle (on-boarding, ongoing assessment, and service or contract termination).				
Maintains inventory of third party vendors assessed for security risk.				
Implements process for assigning risk ratings to new third parties and vendors, and confirms that new third parties and vendors are assigned a risk rating.				
Incorporates standard security requirements in third-party contracts and obtains legal and security guidance on changes to defined requirements.				
Incorporates third party security assessment process into procurement processes.				
Performs operational and third party risk assessments in support of business operations (to include workflow, vendor, application and associated dependencies and controls).				
Promotes oversight and governance in Information Security Governance and Risk Management across business operational areas throughout the university.				
Develops, documents and maintains enterprise-wide policies, standards and guidelines for third party risk management across the university.				
Provides consultation on current business processes to redesign for risk reduction, best practice compliance with regulatory requirements, efficiency and effectiveness.				
Contributes to the enhancement in tools and methodologies used to assess risk and establish guidelines and tools to facilitate continuous improvement in the related initiatives by performing business risk analysis and providing leadership to internal business partners.				
Engages with project teams to strengthen the operational risk posture of the organization and establishes appropriate operational risk and security standards.				
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				

JOB ACCOUNTABILITIES

	<i>% Time</i>	<i>Essential</i>	<i>Marginal</i>	<i>N/A</i>
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: https://policy.usc.edu/mandated-reporters/
<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: https://dps.usc.edu/alerts/clery/			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.