



# Security Risk Management Analyst

## Job Description

### JOB INFORMATION

Job Code:	166067
Job Title:	Security Risk Management Analyst
FLSA Status:	Exempt
Supervisory:	
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

### JOB SUMMARY

Responsible for analyzing documented practices pertaining to risk compliance; monitors compliance actions to ensure systems, data and configuration management are in accordance with internal security, provides comprehensive systems and data analyses that are used to record and maintain security plans. Plays an integral role in internal and external security audits, evaluates proposed changes to all systems, and ensures proper protection and/or corrective measures are taken when incidents or vulnerabilities are discovered.

### JOB QUALIFICATIONS:

#### Education

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

Req	Pref	Work Experience	Experience Level
X		3 years	
	X	5 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

Req	Pref	Functional Skills
X		Understanding of regulatory requirements (e.g., GLBA, PCI, FERPA, HIPAA).
X		Broad breadth of technical skills and experience in IT, security and privacy.

## Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Knowledgeable of information security across all security domains and the relationship between threats, vulnerabilities and information value in the context of risk management.
X		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.
X		Experience performing information security risk assessments and risk analysis.
X		Demonstrates problem-solving skills.
	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	Experienced in presenting to management.
	X	Strong interviewing skills and ability to adapt communication style based on stakeholder preferences.
	X	In-depth experience in system hardening, analysis and vulnerability management.
	X	Proficient in Windows, Linux, and Mac OS.
	X	Experienced in Federated or decentralized environments.

## Other Job Factors

## JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Provides risk mediation, drafts mitigation or escalation plans, and ensures compliance is met. In coordination with the Information Security Advisor team and the Office of Compliance, addresses non-compliance to established information security practices across the University and analyzes plans of action developed with risk owners.				
Establishes and maintains comprehensive systems and data security analyses practices, and uses data taken from ongoing analyses to create concise documentation. Monitors compliance actions within an approved Compliance Tracking system, continually reviewing against regulations, policies and laws related to university business.				
Analyzes data stored in multiple systems to ensure integrity of plans, and adherence to established university security internal security policies and practices outlined in the Information Security Governance and Risk Management (ISGRM) Program.				
Establishes and evaluates configuration management programs for security-relevant software, hardware and firmware for maintenance and documentation, in accordance with the ISGRM Program.				
Develops and oversees relevancy and accessibility of all internal ISGRM information security-related documentation in a knowledge base lifecycle and configuration database. By way of lifecycle review and minor data entry, creates and analyzes records maintained for workstations, software, servers, routers, firewalls, network switches, and equipment; ensures all information system security-related documentation is current and accessible to properly authorized individuals.				
Analyzes and reviews proposed changes and additions to USC's information systems, advising the ISGRM Program of their security relevance, and provides input in internal and external security audits, performing risk assessments as assigned.				
Probes to ensure proper protection and/or corrective measures have been taken when an incident or vulnerability has been discovered.				
Audits Information Systems Security Plans, and develops, implements and enforces Information Security Policies and Procedures together with the ISGRM Program team.				

## JOB ACCOUNTABILITIES

	<i>% Time</i>	<i>Essential</i>	<i>Marginal</i>	<i>N/A</i>
Creates, monitors, analyzes and measures risk treatment activities through the security metrics program.				
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>			Yes

## 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.