



## Senior Analyst, Information Security Risk Management Job Description

### JOB INFORMATION

<i>Job Code:</i>	166066
<i>Job Title:</i>	Senior Analyst, Information Security Risk Management
<i>FLSA Status:</i>	Exempt
<i>Supervisory:</i>	May oversee staff, students, volunteers, agencies and/or resource employees.
<i>Job Family:</i>	IT Security
<i>Job Family Group:</i>	Information Technology
<i>Management Level:</i>	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 policies and practices. 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. Ensures proper protection and/or corrective measures are taken when incidents or vulnerabilities are discovered.

### JOB QUALIFICATIONS:

#### Education

<i>Req</i>	<i>Pref</i>	<i>Degree</i>	<i>Field of Study</i>
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

<i>Req</i>	<i>Pref</i>	<i>Work Experience</i>	<i>Experience Level</i>
X		5 years	
	X	6 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		Understanding of regulatory requirements (e.g., GLBA, PCI, FERPA, HIPAA).
X		Broad breadth of technical skills and experience (e.g., IT, security, privacy).

## Knowledge, Skills and Abilities

Req	Pref	Functional Skills
X		Knowledge 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/regulatory requirements and industry security frameworks.
X		Experience performing information security risk assessments and risk analysis.
	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	Experience presenting to management. Strong interviewing skills.
	X	Ability to adapt communication style based on stakeholder preferences.
	X	In-depth experience in system hardening, analysis and vulnerability management.
	X	Proficiency in Windows, Linux, and Mac OS.
	X	Experience in federated or decentralized environments.
	X	Strong written and oral communication skills.
	X	Technical documentation, training, and instructional design abilities.
	X	Strong interpretive and relationship management abilities.
	X	Knowledge of applicable laws/policies/principles/etc.
	X	Demonstrated proficiency in project management, scheduling, and problem identification and resolution.
	X	Experience with network security and database configuration, administration and management.

## Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		Certified Information Security Auditor - CISA
	X		Certified Information System Security Professional - CISSP
	X		Certified in the Governance of Enterprise IT - CGEIT

## Other Job Factors

## JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Provides risk mediation; drafts mitigation or escalation plans. Analyzes data stored in multiple systems to ensure integrity of plans. Creates, monitors, analyzes and measures risk treatment activities. Develops and oversees all internal governance, risk and compliance information security-related documentation. Creates and analyzes records. Ensures all information system security-related documentation is current and accessible to properly authorized individuals.				
Maintains industry awareness and knowledge of relevant changes; communicates changes to senior management as appropriate. Establishes and maintains appropriate network of professional contacts. Maintains membership in appropriate professional organizations. Attends meetings, seminars and conferences; maintains continuity of any required or desirable certifications, if applicable.				
Ensures proper protection/correction is taken when an incident or vulnerability is discovered. Audits information systems security plans; develops, implements and enforces information security policies and procedures together with the policy team.				
Establishes and maintains comprehensive systems and data security analyses practices; creates concise documentation. Monitors compliance actions. Establishes and evaluates configuration management programs. Ensures compliance with established university security internal security policies and practices; addresses non-compliance and analyzes plans of action developed with risk owners. Analyzes and reviews proposed changes and additions to university's information systems. Provides input in internal and external security audits.				

## JOB ACCOUNTABILITIES

	<i>% Time</i>	<i>Essential</i>	<i>Marginal</i>	<i>N/A</i>
Promotes an environment that fosters inclusive relationships and creates unbiased opportunities for contributions through ideas, words, and actions that uphold principles of the USC Code of Ethics.				

## 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>			

## 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.