



Information Security Governance and Risk Management Director Job Description

JOB INFORMATION

<i>Job Code:</i>	168025
<i>Job Title:</i>	Information Security Governance and Risk Management Director
<i>FLSA Status:</i>	Exempt
<i>Supervisory:</i>	Manages through subordinate supervisors.
<i>Job Family:</i>	IT Security
<i>Job Family Group:</i>	Information Technology
<i>Management Level:</i>	4 Administrator

JOB SUMMARY

Responsible for developing the strategy and vision for the governance and risk management team, and the execution of the responsibilities within the governance and risk management directorate. Accountable for the key governance and risk management areas, including but not limited to, security training and awareness, policy management, information security metrics, data protection, security risk management, information security consulting, third party management, software security and security architecture. Oversees the data protection program, monitors the effectiveness of the security risk management and third party management functions, and oversees the management of the security architecture function, while providing security risk management consulting and structure from a cyber-governance perspective for key stakeholders across the university. Directly or indirectly manages all program staff and develops and administers a budget, while maintaining up-to-date knowledge in the field of specialty.

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		8 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

Req	Pref	Functional Skills
X		Understanding and technical knowledge of key Information Security Governance concepts, including but not limited to security training and awareness, policy management, metrics, and data protection.
X		Understanding and technical knowledge of key Risk Management concepts, including but not limited to security risk management, information security consulting, third party management, software security, and security architecture.
X		Strong technical understanding of enterprise computing solutions including cloud hosting, SAS models and oversight responsibilities.
X		Strong written and executive communication, including up to the C-level.
	X	Experience in the implementation and/or management of Governance, Risk, and Compliance (GRC) technologies and supporting processes.
	X	Experience working in a regulatory environment and working in large or federated enterprises, preferably in the university environment.

Certifications

Req	Pref	Select Certifications	Enter Additional Certifications
	X		CISSP

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	Essential	Marginal	N/A
Serves as a Subject-Matter Expert (SME). Provides expertise and understanding of all aspects of the Information Security Governance and Risk Management (ISGRM) landscape, working with senior leadership to mold and shape the ISGRM footprint.				
Defines an ISGRM strategy, with a roadmap of key deliverables and timelines, and delivers consistently. Leads large cybersecurity initiatives with a focus on risk management and compliance. Oversees the design of best practice solutions and work plans for the University's governance and risk management in collaboration with internal and external resources.				
Oversees the policy, standards and policy exceptions management process and coordinates approval and updates with appropriate parties. Involves relevant parties for security risk and compliance issues that span legal, compliance and regulatory requirements.				
Oversees the data protection program, including assessing the level and quality of service provided by professional services. Evaluates and determines new goals and objectives. Creates, prepares and delivers reports to senior management. Makes recommendations, as necessary.				
Oversees the development and delivery of all security training and awareness campaign.				
Oversees the needs assessment of information consulting for all schools, units and hospitals. Evaluates and determines new goals and objectives. Creates, prepares and delivers reports to senior management. Makes recommendations, as necessary.				
Provides input to the selection of key metrics to monitor and oversees the implementation of metrics capturing, including technology solutions across the university.				
Participates in the development and administration of the department budget. Approves/disapproves department expenditures. Develops short and long-term budget projections and plans. Provides financial status reports as needed.				
Directly or indirectly manages program and administrative staff, usually through subordinate managers and supervisors. Recruits, screens, hires, and trains staff, as necessary. 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. Recommends, approves and monitors professional training and development opportunities for staff.				

JOB ACCOUNTABILITIES

	<i>% Time</i>	<i>Essential</i>	<i>Marginal</i>	<i>N/A</i>
Monitors the effectiveness of the security risk management and third party management functions, including assessing the level and quality of service provided by professional services, including software security and security controls assessment services.				
Oversees the management of the security architecture function and the integration with risk assessment processes and activities across the university.				
Collaborates cross-functionally with other technology teams and security policy organizations. Represents the unit or university on internal and external committees, task forces, or boards, as assigned. Provides consultation across the university to stakeholders concerning risk management and governance.				
Maintains up-to-date knowledge by researching new technologies and software products, participating in educational opportunities and conferences, and reading professional publications.				

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/			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.