USC University of Southern California

Lead Analyst, Information Security Risk Performance

Job Description

JOB INFORMATION

Job Code:	166103
Job Title:	Lead Analyst, Information Security Risk Performance
FLSA Status:	Exempt
Supervisory:	Leads one or more employees performing similar work.
Job Family:	IT Security
Job Family Group:	Information Technology
Management Level:	7 Individual Contributor

JOB SUMMARY

Responsible for leading a risk-based performance management approach to university information security. Develops and implements comprehensive information security strategies and programs to identify and mitigate business risk. Defines and builds key performance indicators to ensure effectiveness and compliance across information security processes and process owners. Assists in managing evaluation process that determines effectiveness of information security controls and safeguards. Ensures processes align to regulatory, statutory, and industry requirements, as well as university policy and data classification. Participates in external and internal compliance audits. Serves as a subject matter expert on information security risk strategy and risk appetite.

JOB QUALIFICATIONS:

Education

Req	*Pref*	*Degree*	*Field of Study*	
X		Bachelor's degree		
X		Bachelor's degree	Information Science	Or
X		Bachelor's degree	Computer Science	
	X	Bachelor's degree	Information Science	Or
	X	Bachelor's degree	Computer Science	

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		2 years	in information security or risk management	
	X	3 years	in information security or risk management	

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		Demonstrated understanding of information security across all security domains and the relationship between threats, vulnerabilities, and information value in the context of risk management.
X		Experience with legal and regulatory requirements and industry security frameworks.
X		Demonstrated understanding of processes, internal control risk management, information security controls, and how they interact together.
X		Experience performing information security risk assessments and risk analysis.
X		Demonstrated strong understanding of regulatory requirements (e.g., GLBA, PCI, FERPA, HIPAA).
X		Ability to communicate and present security risk concisely and effectively in relation to enterprise risk based on the appropriate level of management and stakeholder groups.
X		Demonstrated leadership and problem solving skills.
X		Ability to work closely with business leaders in a high pressure, fast-paced, highly collaborative environment with multiple deadlines and competing priorities.
X		Ability to understand data analytics and dashboarding.
	X	Demonstrated strong knowledge of information security, risk governance, and risk management.
	X	Information security or risk management experience within a large enterprise or complex entity.
	X	Demonstrated data analytics and risk processing skills.

Other Job Factors

JOB ACCOUNTABILITIES

	% Time	*Essential*	*Marginal*	*N/A*
Develops and implements comprehensive information security strategies and programs to identify and mitigate business risk. Obtains input from key stakeholders across university and partners with data protection manager to define annual risk assessment plan. Recommends programmatic direction, with a high degree of independence, in matters relating to the investigation, impact, and analysis of decisions regarding cyber security risk. Creates and maintains key risk indicators (KRIs) and risk appetite in line with the OCISO GRC (governance, risk, compliance) framework. Ensures information security strategies and risk management are performing at established levels.				
Serves as a subject matter expert (SME) on information security risk strategy and risk appetite. Collaborates with risk performance manager to facilitate the risk acceptance process. Ensures the implications of risk acceptance are understood, risks are accepted at the correct level within the organization, and risk acceptances are tracked and reported on throughout their lifecycle.				
Defines and builds key performance indicators (KPIs) to ensure effectiveness and compliance across information security processes and process owners. Specifies key milestones and metrics, as well as associated budget and resource impacts, to continue an effective risk management program. Partners with data protection manager and governance manager to ensure appropriate reporting and data is provided to manage risk.				
Assists in managing evaluation process that determines effectiveness of information security controls and safeguards. Ensures processes align to regulatory, statutory, and industry requirements, as well as university policy and data classification. Participates in external and internal compliance audits (e.g., PCI DSS, HIPAA Security Rule, NIST, GLBA Safeguards). Engages and partners with enterprise and local entities in preparation of compliance audits. Helps track adherence to policy and standards through control evaluation.				
Maintains currency of changes in laws, regulations, and technologies 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. Participates in professional organizations (e.g., attends meetings, seminars, and conferences). Reads pertinent publications. Maintains continuity of any required or desirable certifications, if applicable.				
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

Essential:	*Emergency Response/Recovery*	*Essential:*	*Mandated Reporter*
	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/

Campus Security Authority (CSA)	*Essential:*
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/	

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.