

**CETERA FINANCIAL GROUP
JOB PROFILE**

JOB TITLE:	Information Security Officer		
Job Family:	IT	Job Code:	
Department:	IT	Reports To:	Director, Information Technology
FLSA Status:	Exempt	Location:	El Segundo, CA
Date Completed:	July 14, 2010		

POSITION SUMMARY	<p>The information security officer (ISO) is responsible for establishing and maintaining a corporatewide information security program to ensure that information assets are adequately protected. This position is responsible for identifying, evaluating and reporting on information security risks in a manner that meets compliance and regulatory requirements. The ISO position requires a visionary leader with strong skills in technology and business management. The ISO will proactively work with business units to implement practices that meet defined policies and standards for information security. He or she will also oversee all IT risk management activities.</p> <p>The ISO serves as the process owner of all ongoing activities related to the availability, integrity and confidentiality of customers, business partners, employees and business information, in compliance with the organization's information security policies. A key element of the ISO's role is working with executive management to determine acceptable levels of risk for the organization. The ISO must be highly knowledgeable about the business environment and must ensure that information systems are maintained in a fully functional, secure mode.</p> <p>The ideal candidate is an integrator of people and processes, a thought leader, a problem solver, an effective consultant and should possess solid domain competency in the field of information security by having eight to 10 years of direct experience in a significant leadership role.</p>
-------------------------	--

PRINCIPAL RESPONSIBILITIES	<ul style="list-style-type: none"> • Develop, implement and monitor a strategic, comprehensive enterprise information security and risk management program to ensure the integrity, confidentiality and availability of information owned, controlled or processed by the organization. • Manage the enterprise's security organization, consisting of direct reports and indirect reports (such as individuals in business continuity and IT operations), including hiring, training, staff development, performance management and annual compensation review. • Develop, communicate and ensure compliance with organizational security policies and standards. • Develop and manage information security budgets and monitor them for variances. • Create and manage information security and risk management awareness training programs for all employees, contractors and approved system users. • Work directly with the business units to facilitate IT risk analysis and risk management processes, identify acceptable levels of risk, and establish roles and responsibilities with regard to information classification and protection. • Provide subject matter expertise to executive management on a broad range of information security standards and best practices, such as ISO 17799, CobiT and ITIL. • Provide strategic and tactical security guidance for all IT projects, including the evaluation and recommendation of technical controls. • Liaise with the enterprise architecture team to ensure alignment between the security and enterprise architectures, thus coordinating the strategic planning implicit in these architectures. • Coordinate information security and risk management projects with staff from the IT organization
-----------------------------------	---

	<p>and business unit teams.</p> <ul style="list-style-type: none"> • Ensure that security programs are in compliance with applicable laws, regulations and policies to minimize or eliminate risk and audit findings. (Examples of applicable laws and regulations include the Sarbanes-Oxley Act, the Graham-Leach-Bliley Act and the Health Insurance Portability and Accountability Act.) • Liaise between the information security team and corporate compliance, audit, legal and HR management teams as required. • Create and facilitate the information security risk assessment process, including reporting and oversight of remediation efforts to address negative findings. • Manage security incidents and events to protect corporate IT assets, including intellectual property, fixed assets and the company's reputation. • Coordinate the use of external resources involved in the information security program, including, but not limited to, interviewing, negotiating contracts and fees, and managing external resources. • Develop effective disaster recovery policies and standards; coordinate the development of implementation plans and procedures to ensure that business-critical services are recovered in the event of a declared disaster, and provide direction and in-house consulting in these areas. • Develop business-relevant metrics to measure the efficiency and effectiveness of the program, facilitate appropriate resource allocation and increase the maturity of the security program. • Facilitate business alignment and communications by forming an information security steering committee or advisory board.
--	---

KNOWLEDGE, SKILLS AND ABILITIES	<ul style="list-style-type: none"> • Minimum of eight to 10 years experience in a combination of risk management, information security and IT jobs, preferably in your company's vertical market. • Excellent written and verbal communication skills; interpersonal and collaborative skills; and the ability to communicate security and risk-related concepts to technical and nontechnical audiences. • Must be a critical thinker with strong problem-solving skills. • Knowledge of technological trends and developments in the area of information security and risk management. • Project management skills; financial/budget management, scheduling and resource management. • Ability to lead and motivate cross-functional, interdisciplinary teams to achieve tactical and strategic goals. • Degree in business administration or a technology-related field, or equivalent work- or education-related experience. • Professional certification, such as a CISSP, CISM, CISA or other information security credentials, is preferred. • Proficient with personal computers; experience with productivity software, such as Windows, Microsoft Office software and so forth.
--	--

	<ul style="list-style-type: none">• Knowledge of security and control frameworks, such as ISO 17799, CobiT, COSO and ITIL.• Experience with contract and vendor negotiations.• High level of personal integrity, and the ability to professionally handle confidential matters and exude the appropriate level of judgment and maturity.• High degree of initiative, dependability and ability to work with little supervision.
--	--

ADDITIONAL INFORMATION	<ul style="list-style-type: none">▪ Does the incumbent in this position have direct accountability for staff supervision/management? No▪ Does the incumbent in this position have budget accountability? No▪ Is travel expected to perform this job? A maximum of 10% domestically per calendar year, if necessary.
-------------------------------	---