

# Director Risk & Contingency - SNEI SD

[Sony](#) - San Diego, US-CA (Greater San Diego Area)

## Job Description

Sony Network Entertainment International LLC (SNEI), a subsidiary of Sony Corporation of America, is the premier provider of digital entertainment. Through the Sony Entertainment Network portal, consumers around the world are able to access their favorite digital entertainment conveniently and instantly on their favorite connected devices. SNEI offers the latest and highest quality music, video, and game content through Sony Entertainment Network as well as PlayStation Network while also delivering third-party services. In addition, SNEI provides a compelling consumer experience through innovative content discovery features and a simple user interface that is globally consistent, yet locally relevant.

Director, Security & Risk Management

San Diego, CA

The Director of Security & Risk Management at SNEI deputizes the office of the Chief Information Security Officer (CISO). This individual is a key senior member of the CISO staff, leading a global team of security professionals, in a high profile business function, responsible for providing security assurance in a complex business environment. The right candidate will play a key part of the CISO's succession strategy and will be expected to demonstrate the ability to operationally interchange with the CISO. To that end, the Director will be working very closely with the CISO as the two roles build a commensurate level of confidence, alignment and situational awareness.

The role requires a rare mix of broad, business and technical acumen wrapped in a persona that motivates business leaders, peers, partners, stakeholders and the company's employees to continually act in a way that helps to secure the commercial success and profitability of SNEI. This role clearly requires strong people-management skills, the ability to inspire and lead in a global context and relevant industry credentials.

The main business objective of this role is to deliver an adaptive set of Security and Risk Management services to ensure that the business operates in a risk mitigated, security managed environment and that the company's control and compliance objectives are being met.

The Director will protect and secure revenue and assets against inadvertent loss or theft, ensure that essential business services are protected and available and that operational risk is being proactively identified and mitigated to acceptable levels.

As a leader, the successful candidate brings subject matter expertise to the position. Leadership of a multi-faceted security program requires generalist knowledge but it is likely that he/she will have specific and relevant business and technical skills. Credibility within the team and the vision to craft an integrated strategy depends on the individual's ability to understand, value, and articulate the varied security missions. Along with the CISO, the Director is a key point of contact for senior executive management and will be available to report at senior executive level on matters within their purview. In particular, corporate security, channel security, product development security, regulatory compliance matters, investigations, intellectual property protection, information security, threat management, security architecture and asset protection methodologies.

## **ESSENTIAL JOB FUNCTIONS:**

### **Strategy, Planning and Operations**

- Reporting to the Chief Information Security Officer, this role delivers security and risk management by developing a strategy and a backbone of policy, standards, process, people and technology to assess and mitigate threats to company assets and employees
- Participate as a member of the management team in governance processes of the organization's security strategies
- Lead strategic security planning to achieve business goals by prioritizing pragmatic, layered, defense initiatives and coordinating the evaluation, deployment, and management of current and future security technologies.
- Develop and communicate security strategies and plans to executive team, staff, partners, customers, and stakeholders.
- Develop, implement, maintain, and oversee enforcement of policies, procedures, and associated plans for system security administration and user system access based on industry-standard best practices.
- Define and communicate corporate plans, procedures, policies, and standards for the organization for acquiring, implementing, and operating new security systems, equipment, software, and other technologies.

### **Operational Management**

- Act as advocate and liaison for the company's security vision via regular written and in-person communications with the company's executives, department heads, and end users.
- Work closely with IT department on corporate technology development to fully secure information, computer, network, and processing systems.

- Manage the administration of all computer security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.
- Develop, track, and control the security services annual operating and capital budgets for purchasing, staffing, and operations.
- Ensure that facilities, premises, and equipment adhere to all applicable laws and regulations.
- Recommend and implement changes in security policies and practices in accordance with changes in local or federal law.
- Creatively and independently provide resolution to security problems in a cost-effective manner.
- Assess and communicate any and all security risks associated with any and all purchases or practices performed by the company.
- Collaborate with the CISO, and Human Resources to establish and maintain a system for ensuring that security and privacy policies are met.
- Where necessary, supervise recruitment, development, retention, and organization of security staff in accordance with corporate budgetary objectives and personnel policies.
- Promote and oversee strategic security relationships between internal resources and external entities, including government, vendors, and partner organization.
- Remain informed on trends and issues in the security industry, including current and emerging technologies and prices. Advise, counsel, and educate executive and management teams on their relative importance and financial impact.
- Provide technical consultancy and guidance to the team around major security design and architectural discussions.
  - An experienced and accomplished technologist
  - Demonstrated ability to build, motivate and lead a professional team attuned to organizational culture, yet be innovative and able to develop new initiatives
  - Demonstrated track record of partnering and developing consensus within an organizational climate of diverse operational activities and wide ranging lines of business
  - Demonstrated ability to communicate clearly within all levels of an organization, including briefing executive management as well as operating teams
  - Have a broad network of collaborative industry and peer contacts

- Excellent conceptual and critical thinking skills and sound judgment, with strategic orientation and ability to perform tactically, as required
- Experience in providing technical expertise appropriate to knowledge of risk and cost effective delivery of essential security services
- Demonstrated ability to identify, analyze and evaluate a large volume of information, and to communicate accurately both verbally and in writing, timely recommendations on business and security related risks to the organization with solid focus on detail, as required
- Ability to develop global security strategies keyed to likely risks and in collaboration with organization's stakeholders
- Ability to anticipate, influence and assist the organization to assess and rapidly adjust to changing conditions and trends in a global multi-cultural environment
- Proven track record of leading, managing and developing employees
- Demonstrated knowledge of and experience with international affairs

### **Formal Education & Certification**

- University degree in the field of computer science, risk management or business administration. Master's or PhD. degree in one these fields preferred
- Certifications in one of more of the following - CISSP, CISM, CISA, CPA, CPP.

### **Knowledge & Experience**

- Minimum of 7 years experience and a demonstrated record of success in positions of increasing responsibility within private sector corporate security, security technology or a related public sector organization, including >3 years of experience within a law enforcement/intelligence or related agency and >3 years of experience in a leadership role
- Preferably >3 years experience managing and/or directing an IT and/or security operation.
- Preferably >3 years experience working in the Entertainment Media or Software industry.
- Proven experience in planning, organizing, and developing IT security and facility security system technologies.

- Track record of building out security teams, roles and functions and securing executive sponsorship
- Experience in planning and executing security policies and standards development.
- Excellent knowledge of technology environments, including information security, building security, and defense solutions.
- Considerable knowledge of business theory, business processes, management, budgeting, and business office operations.
- Substantial exposure to data processing, hardware platforms, enterprise software applications, and outsourced systems, including software development tools and digital distribution technology
- Good understanding of computer systems characteristics, features, and integration capabilities.
- Experience with systems design and development from business requirements analysis through to day-to-day management.
- Excellent understanding of project management and governance principles.
- Superior understanding of the organization's goals and objectives.
- Demonstrated ability to apply IT in solving security problems.
- In-depth knowledge of applicable laws and regulations as they relate to security, data protection, industry and regulatory compliance issues.
- Demonstrates experience & knowledge about conducting lawful & ethical investigations in the workplace and for corporate business
- Experience in audit program management and hands on experience of conducting formal technical, physical and administrative Security Audits within organizations.
- Excellent written communication skills - expected to draft and deliver formal policy documents and reports that hit board level
- High level of knowledge & experience pertaining to Disaster Recovery, Business Continuity & Contingency Planning.

- A detailed understanding the calculation of threat, impact & risk to corporate assets
- Excellent working knowledge of relevant legislation in the areas of copyrights, designs and patents, privacy, data compliance, employment law, environmental issues, freedom...

## Company Description

When it comes to everyday life, Sony Electronics is there. Our products electrify the senses - music, video, photos, laughter and sheer emotion. As a consumer, you feel it across our cool products. And as part of our team, you'll feel the excitement of working for the best brand in the world. Step inside Sony Electronics, and watch our Talent at Work extend nearly 60 years of entertainment history. This is life at its creative best. This is Life at Play.

## Additional Information

Posted:

November 30, 2011

Type:

Full-time

Experience:

Director

Functions:

Information Technology, Management, Project Management, Strategy/Planning

Industries:

Consumer Goods

Compensation:

0

Employer Job ID:

23435

Job ID:

2237443

[https://sony.taleo.net/careersection/2/jobdetail.ftl?lang=en&job=23435&media\\_id=24627&src=LinkedIn\\_Slots](https://sony.taleo.net/careersection/2/jobdetail.ftl?lang=en&job=23435&media_id=24627&src=LinkedIn_Slots)