OLIVER WYMAN GROUP

About Oliver Wyman Group

Oliver Wyman Group (OWG) delivers advisory services to clients through three operating units, each of which is a leader in its field. **Oliver Wyman** (www.oliverwyman.com) is the largest part. It is a top-tier global management consulting firm that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, organizational transformation, and leadership development. **Lippincott** (www.lippincott.com) helps clients create, develop, and manage their corporate branding, identity, and image. **NERA Economic Consulting** (www.nera.com) advises corporations, law firms, and government entities on the economics of competition, regulation, public policy, finance, and litigation.

Visit out website for more details about **Oliver Wyman Group**: www.oliverwymangroup.com .

Job specification

Job Title	**ITS Security & Risk Senior Analyst**
Department	**OWG ITS**
Office	**Singapore**
Reports to:	**Robert Kemp**
Hours	**09:00 - 18:00 (or 8 hour period during normal working hours) with additional hours required**

Job overview

As a trusted member of the Information Technology Services team, the ITS Security & Risk Analyst ensures that information security of Oliver Wyman Group within our infrastructure, applications and business processes is continuously improved. This includes proactive review and remediation of the current state of ITS security issues, management processes, tools and activities, and providing recommendations for enhancement where appropriate. Candidates will have broad Information Security skills with a solid understanding of cross functional IT Security areas such as Identity & Access Management, Infrastructure Security, Application Security, Data Protection and experience working with a broader team on security products and services.

Key roles and responsibilities

- Complete security and technology risk related RFP questionnaires from Clients
- Manage Client Audit requests & work with responsible ITS teams to develop mitigation plans and ensure audit finding are addressed and remediated
- Manage logical security processes, controls and lifecycles are followed efficiently and aligned to deliver compliance with security policies
- Act as the point of contact for internal ITS audits, coordinate audit activities, review evidence provided and manage responses for issues identified and published in audit reports
- Coordinate communication with various stakeholders and provide general support on risk & security related issues
- Oversees the planning, management and execution of Security & Risk projects
- Develops remediation strategies to mitigate risks associated with the protection of infrastructure and information assets
- Provide security consulting and technical assistance with the evaluation, selection, initial set-up and secure deployment of new IT systems
- Assesses threats and vulnerabilities regarding information assets and recommends the appropriate security controls and measures
- Assists with development, implementation, and maintenance of organizational information security policies and procedures
- Work with all teams to ensure security vulnerabilities are addressed and remediated effectively and efficiently

Skills and credentials

- Excellent written and verbal communication skills
- Proven ability to examine, improve and execute the organization's existing security risk assessment processes and procedures
- Ability to weigh business risks and enforce appropriate information security measures; excellent documentation and presentation skills; ability to explain information security concepts to audiences outside of the field
- Strong knowledge of current industry Security standards and best practices (NIST, HITRUST)
- Strong technical knowledge in application security, Directory Services (LDAP, AD), Internet/Intranet architecture and design, operating system hardening, vulnerability management and encryption
- Excellent planning & organizational skills
- Excellent customer\client service orientation
- Polished and professional demeanor
- Occasional travel to other offices and firm events

Experience required

- Security Certification (e.g., CompTIA Security+, CISSP, CISM) is a MUST
- Minimum 6 years of experience in information security experience

- A Bachelors' degree in Computer Science, MIS, business or equivalent experience is required. An advanced degree (e.g. MBA with concentration in information systems) is a plus