INFORMATION SECURITY MANAGER

CNS
at Six Degrees

Access dedicated expertise and operational support in managing information security risks, ensuring compliance, and fostering a secure environment to protect sensitive data and mitigate cyber threats.

Cyber security is a broad and multidisciplinary field that encompasses various aspects of technology, risk management, policy, and human behaviour. Given its scale and complexity, all organisations must establish dedicated capabilities or teams to support their cyber security initiatives and ensure tangible returns on investment.

Six Degrees' Information Security Manager service provides operational risk management along with management of your organisation's information security program. The service covers the implementation and management of security controls, monitoring security incidents, conducting risk assessments, and ensuring compliance with policies and procedures.

The Information Security Manager will oversee day-to-day security operations, collaborating with a range of teams to ensure the effective implementation of security measures.

Six Degrees Information Security Manager Service Benefits

Risk management and compliance. The Information Security Manager oversees risk management activities, conducts risk assessments, and ensures compliance with regulations and industry standards.

Board and stakeholder engagement. The Information Security Manager can assist in preparing reports, metrics, and updates for board meetings and stakeholder communications.

Collaboration with cross-functional teams. The Information Security Manager collaborates closely with teams including IT, legal, HR, and compliance. They ensure alignment between security initiatives and organisational requirements, facilitate communication, and coordinate efforts.

Incident response planning and coordination. The Information Security Manager leads incident response planning, establishes procedures, and coordinates response efforts during security incidents.

Industry and regulatory knowledge. The Information Security Manager keeps abreast of the latest industry trends, emerging threats, and regulatory changes. They assist the CISO by providing timely updates and insights, allowing the CISO to stay informed, make informed decisions, and adapt the organisation's cyber security strategy as needed.

Security operations coordination and oversight. The Information Security Manager handles the operational coordination and oversight of security controls, vulnerability management, user access management, and security awareness initiatives.

Supporting CISOs. The Information Security Manager service plays a critical and complementary role in supporting the organisational CISO by handling operational responsibilities and enabling them to focus instead on strategic planning, board and stakeholder engagement, coordination, and oversight.

Secure, Integrated Cloud Services

Six Degrees Information Security Manager Service Available Deliverables

- **Risk assessments:** Conduct risk assessments as agreed in your scope of work and provide the output to you in a report.

- **Remediation plan:** Review and agree the remediation plan from the cyber security risk assessments.

- **Incident response plan:** Deliver and maintain a cyber security incident response plan.

- **Cyber security training plan:** Develop and maintain bespoke cyber security training for your employees.

- **Cyber security training:** Deliver regular cyber security training for your employees.

- **Cyber security awareness:** Develop and maintain cyber security awareness campaigns for your employees.

- **Threat intelligence:** Monitor and analyse cyber security threat intelligence.

- **Major incident management:** May attend cyber security major incident management bridges, as agreed.

- **Root cause analysis (RCA):** Review and approve root cause analysis documentation for cyber security incidents.

- **Cyber security audits:** Conduct regular cyber security audits and manage the remediation.

- **Business continuity:** Develop and maintain disaster recovery and business continuity plans for cyber security incidents.

- **Security policies and procedures:** Produce policy and procedure documents, aligning to business or compliance requirements.

- **Progress reports:** Report to you on progress against the agreed scope.

Why Six Degrees?

Experienced cyber security leaders. Our practitioners have extensive experience across diverse cross-industry backgrounds and have held CISO roles in high-profile organisations. Their credentials include ISO 27001 and 22301 Lead Implementer, ISO 27001 Lead Auditor, and PCI Qualified Security Assessor.

Backed by the full scope of Six Degrees' cyber security capabilities. Six Degrees will use the full capability of our security practice to help organisations to develop a customised cyber security strategy that meets their unique needs through an intelligence, risk, and threat-based approach.

Extensive Industry experience. Our security team makes cyber security a business enabler. We have helped organisations through a broad range of compliance initiatives including GDPR, NIST Cybersecurity Framework, ISO 27001, Data Protection Act and more, alongside industry specific FCA cyber security requirements and PCI DSS.

Real-world cyber security experience. Our team has a breadth of real-world experience at the board and operational level, guiding organisations through business-impacting cyber incidents and complex business and security transformational programmes into streamlined business as usual operations.

Our Credentials

Member of Microsoft Intelligent Security Association
Microsoft

Assured Service Provider
in association with National Cyber Security Centre
CHECK Penetration Testing

CREST

THE CYBER SCHEME
OFFICIAL CYBER SCHEME SPONSOR

CERTIFICATION BODY
CYBER ESSENTIALS PLUS

ISO 27001

CNS at Six Degrees

For more information about our Information Security Manager service, please contact sales@6dg.co.uk or call 0800 012 8060.