Role Purpose of Senior Manager, Cyber Security

The Senior Manager - Cyber Security is a key management role based in Singapore. Reporting directly to the Asia CISO, the incumbent will be a core member of the Asia Regional Office (ARO) Information Security team. The role will also align to the global cyber security operations team acting as the local leader and influencer for cybersecurity operations across the Asia market. The position is responsible for meeting and maintaining statutory, financial, regulatory and corporate governance compliance obligations with respect to cyber security controls, services and operations managed by the ARO CISO Cybersecurity function.   
  
Accountabilities   
  
Nature of work   
  
Management of cyber security function responsible for defining, developing, updating, and delivering the service for Aviva Asia.   
Leading a dynamic team of cybersecurity specialists responsible for the management, operation and support of security solutions and tools used by the market.   
Drive and manage effective and efficient utilization of existing Cybersecurity tools, processes, licenses and resources.   
Proactively identify, prevent and manage cyber security threats, vulnerabilities and incidents.   
Own cyber security incident management including ‘monitoring, identification, triage, response and recovery’ management.   
Leading the continual uplift and improvement of security tools, controls and supporting processes through cyber transformation activities.   
Engage support and influence technology leadership, business management, 2nd Line Risk and Audits understanding in relation to cybersecurity operational controls and external threat landscape.   
Manage the development, planning (life-cycle) and implementation and availability of cybersecurity technical services and tooling.   
Lead and support global and local initiated cybersecurity related transformation activities to align and uplift local security operations.   
Support, align and work closely with global security operations & threat intelligence teams.   
Establish and maintain expertise in a wide variety of security technologies.   
Ensure Compliance with any AVIVA group standards and related local legislation / frameworks and guidelines, such as the Singapore’s Cybersecurity Act, Singapore’s Personal Data Protection Act, MAS Technology Risk Management guidelines (TRM).   
Collaborate and partner with the ARO CISO Departments leadership team to help define and drive the direction and development of broader function.   
Plan, prioritize and conduct cost analysis for future technical services and tooling to deliver the global security strategy and roadmap   
Provide and support a range of technical security services to Asia market   
Upkeep knowledge of hacker methodologies and tactics (TTPs), system vulnerabilities and key indicators of attacks and exploits.   
Manage identification and resolution of security risks and issues in agreed and timely manner   
Support and achieve Key Performance Indicators and targets for activity, ensuring suitable methods of reporting are in place to link into CISO reporting requirements   
When required act as the deputy to the Asia market CISO providing senior leadership engagement and management coverage support to the broader local CISO team as required.   
Risks & Controls   
  
Identify, own and manage the specific key risks and/or IT controls and Business Protection standards that you are identified as the owner and/or nominee for on iCARE ( GRC Tooling ) or Archer (IT Controls ).   
Ensure that issues and actions associated to controls / risks are remediated in a timely manner   
Maintain appropriate records on iCARE ( GRC Tooling ) or Archer ( IT Controls ).   
Ensure that controls are sufficiently well designed and operating effectively to keep the risks that they mitigate within Aviva's tolerance level   
Report and escalate the status of the relevant risks, controls and standards as appropriate   
Resource Complexity   
  
Accountable for managing a team with people management accountability including recruitment, setting goals, performance management, recommending reward and/or bonus.   
Accountable for agreeing an annual plan and decisions required to deliver an annual cost budget as part of the Asia CISO department.   
Manage to the agreed budget and provide correct information to the planning and time recording tools for recovery of costs.   
Ensure direct team are focused and any performance issues are addresses quickly.   
Mentor and coach team and provide support to peers within Asia CISO.   
Support and guide community new joiners, familiarizing them with the functions processes, toolkit and frameworks.   
Keep abreast of information security frameworks and methodologies (e.g. NIST, ISO) and other information security related best practice appropriate to your role.   
Problem Solving   
  
Address day to day, ad-hoc issues and problems.   
Deal with issues and problems (relating to technical work, people, finance, implementation of change) that are not routine.   
Problem solving may require information gathering, analysis, consideration of options and drawing conclusions on a case-by-case basis.   
Guidelines and policy can help but at the heart of the role is the exercise of judgment based on professional training and/or experience.   
Measure and demonstrate that lessons are learned on issues and repeat incidents are not experienced.   
Know when to escalate and drive resolution to guarantee timely customer expectations.   
Change   
  
Accountable for identifying, anticipating and driving change to secure performance in their service area.   
Changes to the structure and working patterns of the team, to the application of the approved budget, to work processes are likely to be core to the role (while subject to policy and delegations of authority).   
Leaders are accountable for developing the capability of their team and their people and for driving the culture of the organization.   
Internal Collaboration   
  
Collaborate with key users of the service supplied   
Build effective working relationships and influence across CISO, other IT functions across all levels and markets   
Share recent insights and lessons learnt with the wider community through active participation in community discussions   
External Interaction   
  
Build effective working relationships with suppliers, negotiate within budget and contract constraints to make best use of services provided into Aviva   
Seek exposure to third parties in Aviva’s and other industries to share learning; attend key industry events and forums   
Seek opportunities and attend external and internal seminars/ conferences / training sessions that would enhance professional development and deliver business value   
Skills and Qualifications   
  
Bachelor’s degree in a related field such as Computer Science, IT or a Cyber-Security related field   
Minimum of 10-years of professional work experience in the cyber security field, with experience in Managed Security Services and Security Operations environment (Banking and or Insurance experience preferred).   
Certifications in CISSP, SAN GIAC Certifications (GCIH, GPEN, GSEC, etc.), will be advantageous   
Demonstrates good knowledge of cybersecurity technologies, trends, strategy and current legislation and regulations.   
Possesses strong analytical skills to define risk, identify potential threats, and develop action/mitigation plan.   
Possesses strong organizational and project management, interpersonal and communication skills (verbal and written), ability to mentor/train staff and bring awareness to current and emerging threats.   
Ability to manage and prioritize multiple tasks and projects and assist/advise support engineers in establishing appropriate priorities as well as demonstrated ability to manage customer projects and portfolios.   
Develop and maintain comprehensive understanding of Cyber security services and processes managed for market and aligned to global security operations.   
Maturity and presence to support and act as the deputy CISO when required.