Indian Financial Technology & Allied Services

Job Description

I	**Role Summary**	Mandatory

(a) Title:	Senior Manager - Risk and Compliance
(b) Business/Function:	Risk and Compliance
(c) Level:	Senior Manager
(d) Location:	Mumbai
(e) Reports to:	CISO
(f) Team:	Lead the team of 7 members
(g) Summary:	Candidate will lead the IT Risk Management, IT Compliance and Internal Audit in IFTAS. Cloud Security experience is desirable.

II Additional Information

(a) Responsibilities:	1.Lead the ISO 27001 Implementation and ensure its compliance. 2.Based on ISMS monitoring results, evaluate & recommend for Information Security Policy change. 3.Standardization IT and Cyber Security practices as per ISO 27001 and another global standard. 4.Establish acceptable limits for the application, network, or system usage in IFTAS. 5.Ensure security review of the new requirement / projects are performed to ensure required security controls are incorporated. 6.Team is responsible to conduct security review of IT Application / Infrastructure and provide the recommendations for improvement, the review includes hardening, access controls, privilege access, obsolete configuration, etc. 7.Team is responsible to conduct risk assessment of Asset / Service and provide recommendation with remediation steps. 8.Review MSA/SoW/NDA, Contractual requirements of customers and vendors and advise on information security compliance. 9.Facilitate Internal and external audit and track the findings for timely closure. 10.Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. 11.Monitor and evaluate the effectiveness of IFTAS Information Security controls / safeguards to ensure that they provide the intended level of protection. 12.Create Policies, Processes, and Standards. 13.Develop methods to monitor and measure risk and compliance. 14.Develop methods for Internal and third-party audit (e.g., cloud service providers, data centers). 15.Ensure information security requirements are incorporated in new IT Procurement / Outsourcing. 16.Ensure that Production and Non-Production (UAT, Testing) environments follow Information Security Policy. 17.Ensure that Information / Data Protection controls are implemented as per Information Security Policy. 18.Identify, assess, and recommend cybersecurity controls or cybersecurity-enabled products for IFTAS. 19.Adhere and promote the information security policy awareness and best practices in the company.

III	**Requirements**	Mandatory

(a) Education:	1) Graduate - Any stream 2) Security management Certifications like CISA / CISSP / CISM is must
(b) Experience:	Candidate must have 12+ years of total experience with 7-9 years' of relevant experience
(c) Knowledge:	1.ISO 27001 and PCI DSS Standards & Controls 2.Drafting / implementing Information Security Policy 3.IT Risk Management and IT Compliance 4.IT, Cyber Security best practices, processes, and tools 5.Cloud Security best practices
(d) Skills:	IT Security Information Security CISA CISM