JOB DESCRIPTION

ISO 27001 implementation and Certification

Scope of Work

1. **Assist Directorate's Chief Information Security Officer (CISO) to:**
    a. Conduct Gap Analysis for ISO 270001/ISMS implementation
    b. Conduct Risk Assessments and suggest Mitigation plans/Controls
    c. Conduct /Assist in VAPT and assist in closure of Vulnerabilities
    d. Prepare of Policies and Processes
    e. Prepare Training Plan
    f. Train the Stakeholders
    g. Conduct Mock Audits
    h. Assist in ISO 27001, final Audit

Roles and Responsibilities:

1. Assist CISO in the implementation of the Information Security Management System based on the ISO/IEC 27000 series standards, including preparation for certification against ISO/IEC 27001.
2. Perform gap analysis of information security standards such as ISO 27001:2013 and create compliance reports for information security standards such as ISO 27001:2013 and other requirements (IT Act/CII)
3. Leads the preparation and the implementation of necessary: Information security policies, standards, procedures and guidelines, in discussion with the departments CISO/ Information Security Committee, to get appropriate approvals and feedback, for implementation.
4. Manages and leads the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies etc. and applicable laws and regulations ((IT Act, NCIIPC guidelines, Critical Information Infrastructure controls etc)
5. Support department and help manage implementation of information security management system.
6. Conduct Information security awareness, training and educational activities to stakeholders.

7. Manages information security risk assessments and controls selection activities
8. Liaison with stakeholders and offers strategic direction to related governance functions (such as Risk Management, IT, HR, Legal and Compliance)
9. Liaison with senior and middle managers throughout the project organization as necessary, on information security matters such as routine security activities plus emerging security risks and control technologies
10. Present reports and recommendations to CISO on information security and related issues
11. Work independently under the general direction of the CISO to ensure timely and accurate completion of information security internal audit objectives and perform the requisite preparation
12. Manage Third Party Security Assessment Program to minimize risk associated with business partners and vendors.
13. Perform testing of internal controls specified in Information Security Policies and Perform internal audit reviews to assess the effectiveness of current information security controls
14. Ensure timely and effective corrective actions are taken to correct deficiencies and provide status reporting.
15. Support the Information Security program including development, collection, assessment, and reporting of metrics
16. Recommend security policy changes and enhancements as needed and assist CISO in implementation
17. Conduct Mock ISO Audits and, Report on departments preparedness for final audit and certification
18. Assist CISO in ISO 27001- Audit and certification

Qualifications:

1. Should have Bachelors/Master's degree and hold professional certification viz., CISA, CISSP/ CISM, CRISC etc., ISO 27000 – Implementer/Lead Auditor etc,
2. Should have led at least Two implementation of ISMS and one implementation as Lead Auditor.
3. Should have led One implementation of BCMS
4. Broad-based IT experience with technical knowledge of Networks, Hardware, Storage, Operating systems, and Applications, Business Impact Analysis, RTO/RPO, Communication Plan, ITDR Drills, Contingency Plans etc

5. Up-to-date understanding of emerging trends in information security and apply new techniques and trends, in-line with overall information security objectives and risk tolerance
6. Good writing skills for Policy & Procedures, BCP documentation
7. IS Awareness, Training and Assessment: Preparing Training plans and conducting relevant Trainings for stakeholders
8. Experience in working on Cyber Security Projects of Government/ Industry

S.No.	Description	Details
1.	Date of Issuance	8th January 2018
2.	Date and time of Submission of Application	10th January 2018 Before 05:00 pm
3.	Mode of Submission (e-mail)	To: triveni.mehta@nisg.org copy to: sanjay.bobde@nisg.org srinivas.j@nisg.org@nisg.org
4.	Contact person for clarifications	Dr.Srinivas Josyula (srinivas.j@nisg.org@nisg.org) 09701933318