भारतीय प्रबंध संस्थान बेंगलूर
INDIAN INSTITUTE OF MANAGEMENT
BANGALORE

Ref: IIMB/HR/RECT/2024/30 Date: 02 May 2024

About IIMB	The Indian Institute of Management Bangalore (IIMB) is a leading graduate school of management in Asia. Underthe IIM Act of 2017, IIMB is an Institute of National Importance.
Industry/Service	Higher Education
Post/Job Title	**Manager - Cybersecurity & Compliance**
Job Purpose	The Cybersecurity & Compliance Manager will be the primary staff responsible for the IT security of IIMB. Will be providing strategic leadership and direction (like a CISO) in developing and implementing comprehensive cybersecurity programs. This role requires a seasoned professional with a deep technical and managerial understanding of cybersecurity, risk management, and compliance (ISO, CERT.in, etc.). The ideal candidate will lead efforts to protect the organization's information assets, ensure regulatory compliance, and respond effectively to cyber threats.
Job Type	Contractual – Non-Teaching
Reporting to	ITFAC Chairperson
Will also closely work with	All relevant stakeholders of the Institute
Principal Accountabilities & Responsibilities	• Strategic Leadership: Develop and execute a comprehensive cybersecurity strategy aligned with organizational goals and industry best practices. Provide strategic guidance to senior management on cybersecurity risks and mitigation strategies in coordination with Manager IT operation & team. • Governance and Compliance: Rewrite, establish and enforce cybersecurity policies and procedures to ensure compliance with industry standards and regulations, especially ISO and CERT.in. Oversee the development and maintenance of security frameworks and controls. • Risk Management: Conduct regular risk assessments to identify, prioritize, and mitigate cybersecurity risks. Work with cross-functional teams as well as external auditors and consultants to integrate risk management into business processes. Conducting vulnerability assessment tests and identifying and addressing any weaknesses. Identifying social engineering and phishing risks. • Incident Response and Recovery: Lead the development and implementation of an effective incident response and recovery plan. Manage and coordinate responses to cybersecurity incidents, ensuring timely resolution and minimizing impact. Prepare information security performance report based on results from analysis and correlation of information security events. • Security Awareness and Training: Implement a robust cybersecurity awareness and training program for employees at all levels. Foster a culture of security awareness and compliance within the organization. Develop a documented action plan containing policies, practices and procedures that mitigate the identified risks. Document information related to IT security attacks, threats, risks and controls. • Technology Integration: Evaluate existing IT environment against organization's IT strategic directions. Collaborate with IT and technology teams to integrate cybersecurity measures into new and existing systems. Stay abreast of emerging technologies and threats, advising on their implications for the organization. • Security Architecture: Managing, deploying and maintaining security infrastructure. Overseeing the design and implementation of secure information systems architecture. Ensure the organization's infrastructure is resilient against evolving cyber threats. Implementing security systems, such as firewalls, data protection controls and encryption.

	• Budget and Resource Management: Develop and manage the cybersecurity budget, ensuring optimal allocation of resources. Identify and prioritize cybersecurity initiatives based on risk assessments and business needs. Assess operational and implementation costs and evaluate them against the potential business impact if the policies and controls are not implemented.
Key Skill and Ability Requirements	• Excellent technical knowledge of cybersecurity principles, technologies, and best practices. • Strong CISO-equivalent leadership and strategic planning skills to lead IT security of IIMB. • Exceptional verbal and written communication and stakeholder management skills. • Advanced problem-solving and decision-making abilities.
Qualification and Personal Profile	• Education: Master's degree in computer science, Information Security, or a related field. Relevant certifications (CISSP/CISM/CRISC, etc.) are highly desirable. • Experience: Candidate with 8 years' experience, preferably in the field of Cyber security management. Proven experience in developing and implementing successful organization-wide cybersecurity programs.
Compensation	The indicative annual CTC will be in the range of Rs. 13.2 Lakhs to 14.5 Lakhs. The compensation will be fixed based on candidates experience and qualification and will be as per IIMB Contract Appointment Rules

Interested candidates may fill the application using the link: here

The closing date for applications is 16th May 2024. Only shortlisted candidates will be intimated. It is mandatory to fill in all the fields in the application and relevant supporting documents are to be uploaded. Incomplete applications will not be considered.