Job Title: SAP Security Manager
Location: Bangalore

ABOUT UNILEVER:
Be part of the world’s most successful, purpose-led business. Work with brands that are well-loved around the world, that improve the lives of our consumers and the communities around us. We promote innovation, big and small, to make our business win and grow; and we believe in business as a force for good. Unleash your curiosity, challenge ideas and disrupt processes; use your energy to make this happen. Our brilliant business leaders and colleagues provide mentorship and inspiration, so you can be at your best. Every day, nine out of ten Indian households use our products to feel good, look good and get more out of life – giving us a unique opportunity to build a brighter future.
Every individual here can bring their purpose to life through their work. Join us and you’ll be surrounded by inspiring leaders and supportive peers. Among them, you’ll channel your purpose, bring fresh ideas to the table, and simply be you. As you work to make a real impact on the business and the world, we’ll work to help you become a better you.

At HUL, we believe that every individual irrespective of their race, colour, religion, gender, sexual orientation, gender identity or expression, age, nationality, caste, disability or marital status can bring their purpose to life. So apply to us, to unleash your curiosity, challenge ideas and disrupt processes; use your energy to make the world a better place. As you work to make a real impact on the business and the world, we’ll work to help you become a better you!

Unilever’s Cyber Security organization is a multi-disciplinary team responsible for protecting the Confidentiality, Integrity and Availability of our Information and Operations. Our Cyber Security organization runs a 24x7 Security Operations Centre (SOC), oversees a robust Security Architecture and associated technology landscape, provides Cyber Security Solution Engineering and Risk Advisory to our business, and assesses the security of our vast technology estate, including factories, to name but a few areas. Cyber Security sits as part of the Business Operations organisations, as a peer to Unilever’s Technology and Data functions and the broad Supply Chain agenda. Cyber Security is tasked with elevating, reporting on and influencing enterprise cyber security risk mitigation across Unilever. The Cyber Security function is made up of the Governance, Risk, Assurance, and Compliance (GRAC) team, the Tech & Ops team, the BISO teams, and the Office of the CISO.

Role Purpose:

This SAP Security Manager role is tasked with securing our SAP systems globally. This includes cyber risk assessment covering our SAP estate, including for third parties, and representing to the Enterprise Application teams our central security services, applying those services to determine gaps in the security posture and consulting on appropriate risk mitigation approaches, managing security exceptions and participating in cyber incident response where relevant. The aim will be frictionless security, enabling the business to achieve their output and uptime goals through cyber resilience and a strong cyber security culture. These activities will be conducted with a ‘Risk Based’ approach to help individual businesses manage cyber risk in their area.

Role Summary:

A vacancy exists for an SAP Security Manager role within Unilever’s cyber function. The successful candidate will be responsible for the security of our SAP systems globally. This management position will report to the Information Security Lead for Enterprise Applications (under the Technical Information Security Officer within Tech &Ops) and will work closely with our Enterprise Applications and Enterprise Architecture teams.

Key areas under this role within the Tech & Ops team include:
Cyber security solution engineering and risk advisory for our SAP systems globally, assuring appropriate risk identification, assessment, mitigation, and reporting.

Ensuring the deployment and running of security tooling, in conjunction with the Tech & Ops team.

Advising on security best practice on cyber elements of business initiatives where relevant to SAP security.

Tailoring cyber training and awareness in alignment and partnership with the Cyber Training and Awareness Lead.

Playing an active role in the definition and iteration of the Unilever Cyber Security transformation where relevant to SAP security.

Continuously explore and implement cost effective measures to optimize security investment where relevant to SAP security.

Maintaining and effectively directing the timely closure of security exceptions while reporting status to the Governance, Risk, Assurance and Compliance (GRAC) team.

Providing standards and controls feedback, based on local implementation requirements to the GRAC team to help shape global policies and standards.

Influencing a broad range of stakeholders in various teams across the business, including IT architects, developers and engineers, programme managers, and business data owners where relevant to SAP security.

Define As-Is and To-Be state for SAP security while working in close partnership with Enterprise Architecture, Security Architecture and Enterprise Applications teams.

Main Accountabilities

Responsible for securing our SAP systems globally.

Responsible for advising on security best practice on cyber elements of business initiatives where relevant to SAP security.

Responsible for playing an active role in the definition and iteration of the Unilever Cyber Security transformation where relevant to SAP security.

Responsible to continuously explore and implement cost effective measures to optimize security investment where relevant to SAP security.

Review and develop capabilities in the following SAP GRC modules - Access Request Management (ARM), Access Risk Analysis (ARA), Emergency Access Management (EAM), Segregation of Duty (SoD) and Sensitive Access Rules in ARA.

Responsible for managing Risk and Access Controls within the SAP landscape and working closely with Enterprise Security Architecture and Internal Audit teams.

Responsible for ensuring technical governance is based on sound architectural principles and correctly documented.

Responsible for reviewing the Security Notes with SAP platform teams.

Responsible for working with multiple teams to facilitate decision making for critical cyber risk in the Unilever SAP technology space.

Responsible for working closely with Cyber Standards and Controls team to define and modify SAP application baseline controls.

Responsible for working closely with the Security Engineering team in the deployment of new security tools and governance of existing global security tools in the SAP estate.

Responsible for owning Unilever SAP Security best practice documents and providing guidance to BISOs for local IT and regional SAP solutions.

Key Skills and Relevant Experience

Skills:

Excellent written and verbal communication skills and able to be understood by both technical and non-technical personnel.

Proven ability to lead, develop, and motivate a team.

The ability to lead through accountability with delegated responsibilities.

Ability to manage conflicting priorities and multiple tasks.

Stakeholder management and interpersonal skills at both a technical and non-technical level.

Outstanding influencing ability.

Able to work in a collaborative environment with international team members.

Outstanding critical reasoning and problem-solving skills – sticking to the problem until it is resolved.

Customer-orientated, whether responding to queries or delivering new services.

Skills in Programme and Project Management.

Experience:

The role holder will have previously held a role in Cyber Security, with specific experience in SAP (or similar systems) security.

Technical knowledge of SAP security architecture and role-based authorization models for relevant SAP systems (ECC, BW, GRC, Solution Manager etc.) is required.

Solid understanding in SAP Security tables is required, and the ability to efficiently and accurately identify authorization errors to provide consultative support to the wider organisation.

Familiarity with API Security and SAP integration technologies - PI, XI, BODS.

SAP Certified Technology Professional preferred.

Experience with Azure cloud hosting and security best practice is a plus.

Experience or knowledge of control frameworks, such as Sarbanes Oxley is a plus.

Extensive experience in providing thought leadership, and driving a complex change agenda, and an ability to challenge the “status quo”.

Excellent strategic and operational business awareness, with a deep understanding of the key drivers, levers, issues and constraints of digital businesses.

Experience within a customer focused environment.

Knowledge of the applications or the technical landscape within the domain and experience of delivering Cyber Security projects to its demands.

Behaviours

Candidates would be required to demonstrate the Unilever Standards of Leadership & live the Values through showing the following behaviors:

Agility – Flexes leadership style and plans to meet changing situations with urgency. Learns from the past, envisions the future, has a healthy dissatisfaction with the status quo.

Personal Mastery – Actively builds wellbeing and resilience in themselves and their team. Has emotional intelligence to take feedback, manage mood and motivations, and build empathy for others. Sets high standards for themselves and always brings their best self.

Passion for High Performance – Inspires the energy needed to win, generating intensity and focus to motivate people to deliver results at speed.