

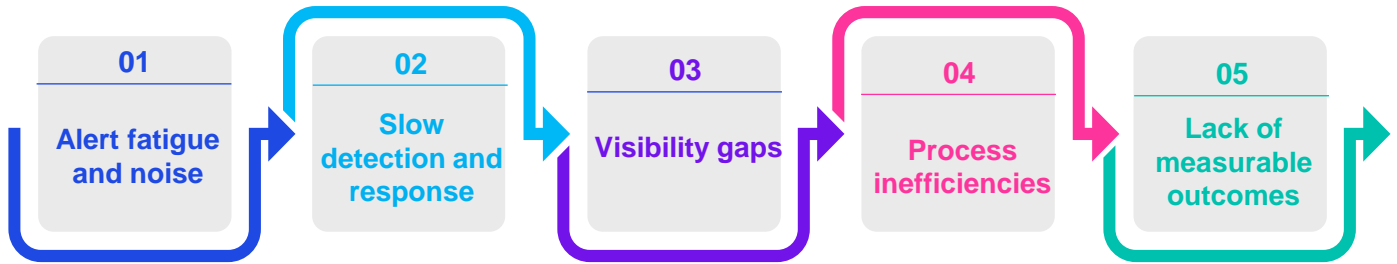
Stop playing defense - optimise your Security Operations Center (SOC) for real impact

A KPMG in India service for SOC efficacy and maturity



The SOC challenge - investment ≠ effectiveness (key pain points)

Many organisations have invested heavily in SOC technology (SIEM, SOAR, EDR/XDR) and people, but without maturing the underlying processes, governance, and service delivery, the full value of those investments remains untapped.



Confidence in your SOC starts with clarity—do you truly know how well it can detect, respond, and adapt when it matters most?

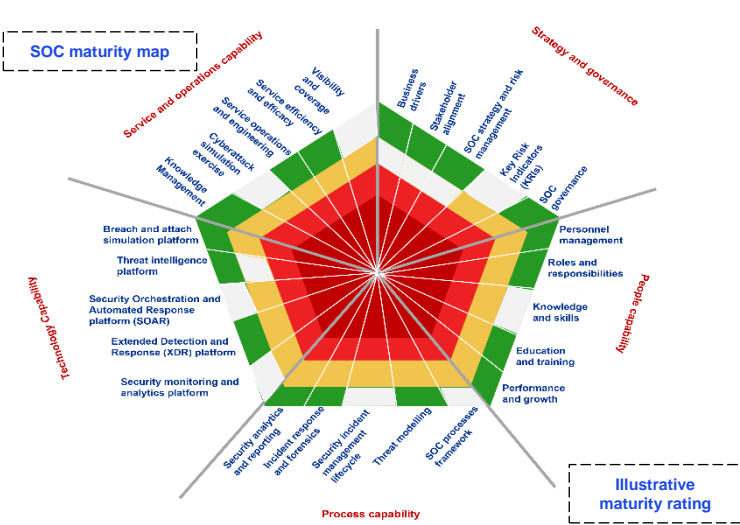
01
If your **internal attack surface** is targeted today, would you be able to detect it — or only react after a breach?

02
When was the last time your SOC **effectiveness** was **objectively measured** against industry peers and evolving threats, not just internal SLAs?

03
Do you have **board level confidence** that your SOC can handle not just today's threats, but AI-powered attacks?

04
Are your compliance reports **masking critical SOC capability gaps** that could become catastrophic liabilities after your next audit?

SOC maturity tiers¹



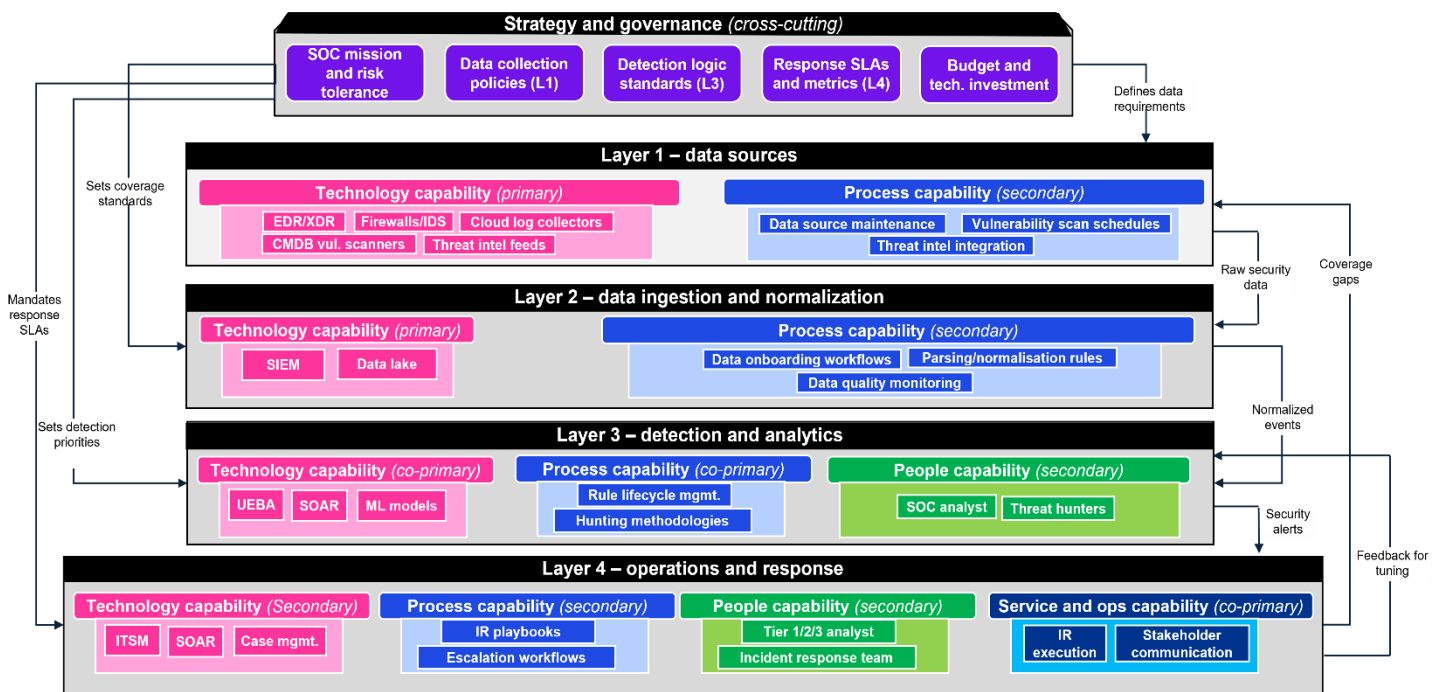
- Maturity level 1** **Absent:** Not implemented at all.
- Maturity level 2** **Initial:** Ad-hoc and unpredictable. Success depends on individual heroics.
- Maturity level 3** **Managed:** Some processes and capability are repeatable; Process discipline often reactive.
- Maturity level 4** **Defined:** Process standardized; Process discipline in place to repeat earlier success; Documented and delivered consistently.
- Maturity level 5** **Quantitatively Managed:** Systematically measures for quality and consistency; feedback loop present for few.
- Maturity level 6** **Optimizing:** Optimized and continuously improved program; Helping self and community.

How KPMG in India can help?

At KPMG in India, we recognise the complexities organisations face in strengthening their SOC to effectively detect, respond to, and mitigate cyber threats. To address these challenges, we help organisations evaluate the effectiveness and maturity of their SOC against industry standards and leading practices. Our SOC maturity assessment framework provides:

- Thorough evaluation of SOC capabilities across people, process, technology, service, strategy and governance
- Gap analysis and benchmarking against global frameworks and threat landscapes
- Actionable recommendations to enhance detection, response, and resilience
- Roadmap for maturity improvement aligned with business and compliance objectives.

Mapping SOC architecture to five SOC maturity domains



SOC efficacy assessment framework²

SOC area	Business drivers	Stakeholder alignment	SOC strategy and risk mgmt.	Key Risk Indicators (KRIs)	SOC governance
Strategy and governance	<ul style="list-style-type: none"> Business requirements Requirements updates Risk identification Asset inventory Risk & asset updates. 	<ul style="list-style-type: none"> Stakeholder mapping Information requirements Service updates Stakeholder feedback, satisfaction tracking Service contracts, escalation paths. 	<ul style="list-style-type: none"> SOC charter Charter awareness SOC mandate Security policies Retention policy, retention setup SOC policy. 	<ul style="list-style-type: none"> KRI threshold documentation Privacy incident correlation KPI-KRI alignment. 	<ul style="list-style-type: none"> Governance process, meeting cadence, metrics-driven governance, cost management, budget forecasting, internal audits, RACI approval, risk-based decisions.
People capability	<ul style="list-style-type: none"> Personnel management Onboarding process Background checks Coaching & evaluation Career pathways Satisfaction tracking Termination process. 	<ul style="list-style-type: none"> Roles and responsibilities Role definitions Recruitment alignment. 	<ul style="list-style-type: none"> Knowledge and skills Knowledge process Knowledge matrix Gap resolution Knowledge sharing platform. 	<ul style="list-style-type: none"> Education and training Training program Certification program Training resources Staff certification. 	<ul style="list-style-type: none"> Performance and growth Recruitment process Talent strategy.
Process capability	<ul style="list-style-type: none"> SOC process framework and detection eng. SOC management Detection process Process metrics MITRE ATT&CK® testing Playbook testing Ti-based testing. 	<ul style="list-style-type: none"> Threat modelling Use case process and docs, change control, use case review, effectiveness metrics, risk-based use cases, threat intel usage, PR UC-B – MITRE ATT&CK® mapping, MITRE ATT&CK® gap analysis, MITRE ATT&CK® profiles. 	<ul style="list-style-type: none"> Security incident lifecycle mgmt. Incident process, standards-based, service metrics, service onboarding, service offboarding, incident tracking, incident prioritization, incident escalation, closure reasons, post-incident review, incident reports, detection enhancement. 	<ul style="list-style-type: none"> Incident response and forensics Response plan, incident communication, remediation actions. 	<ul style="list-style-type: none"> Security analytics and reporting Metric-based reports Report delivery Content approval Threat advisories.
Technology capability	<ul style="list-style-type: none"> Breach and attack platform simulation Platform documentation Coverage monitoring. 	<ul style="list-style-type: none"> Threat intelligence platform Platform ownership Task automation. 	<ul style="list-style-type: none"> SOAR platform Change control Access control. 	<ul style="list-style-type: none"> XDR platform Detection architecture Support readiness. 	<ul style="list-style-type: none"> Security monitoring and analytics platform Continuity planning Secure ingestion. Ingestion monitoring.
Service and operations capability	<ul style="list-style-type: none"> Knowledge management TI process, TI procedures, source collection Standardized sharing, TI analysis TI reports, stakeholder sharing. 	<ul style="list-style-type: none"> Cyber attack simulation exercise Hunting process, service metrics Hunting procedures, detection improvement, intel-driven hunting, IOC detection, artifact detection, TTP detection. 	<ul style="list-style-type: none"> Service operations and engineering Monitoring process, service metrics, service onboarding, service offboarding, event analysis, lifecycle detection, multi-stage detection, threat intel usage, false positive management. 	<ul style="list-style-type: none"> Service efficacy and efficiency Service metrics Service onboarding, service offboarding. 	<ul style="list-style-type: none"> Visibility and coverage Environment coverage Threat coverage.

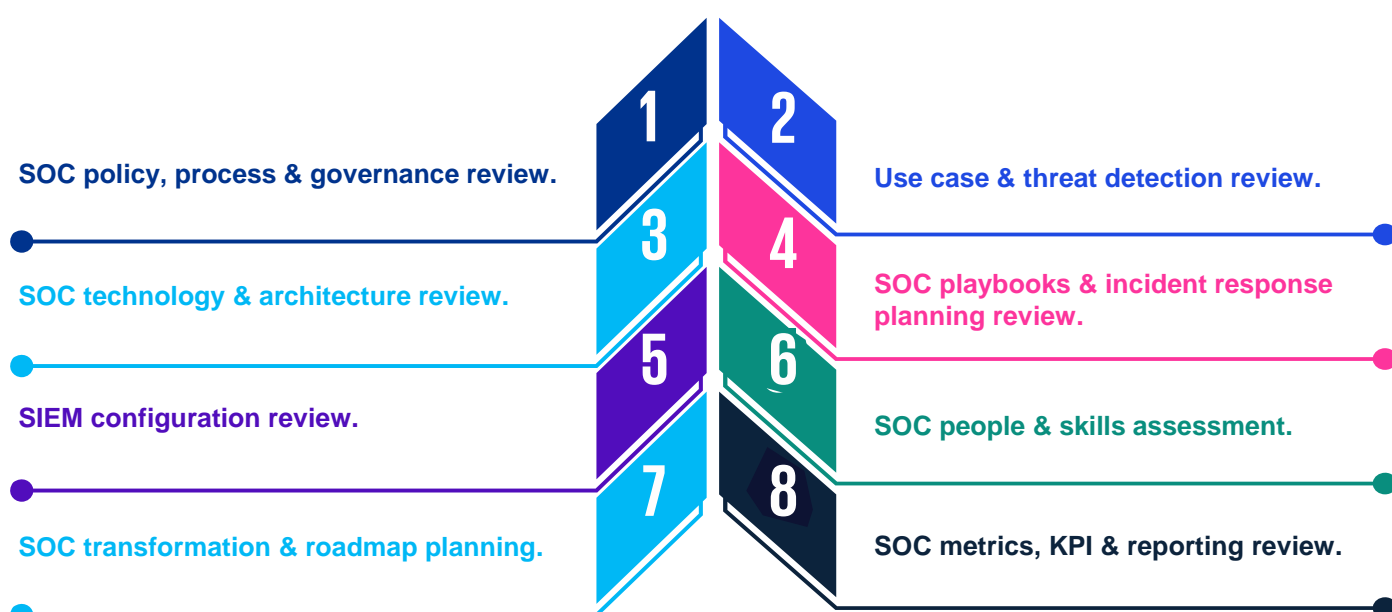
²SOC –CMM certification scheme, SOC CMM, October 2024

Our approach

SOC efficacy & maturity assessment provides a structured evaluation of the SOC's current capabilities across business, people, processes, services, strategy and governance and technology. This assessment benchmarks maturity against industry standards, identifies control and operational gaps, and delivers actionable recommendations with a phased roadmap for improvement. We shall tailor our approach to your specific environment, leveraging our experience in delivering similar advisory projects across industries.

1	Understand	Conduct project kick-off and finalize the scope including in-scope locations, teams, technologies, and processes.
2	Control framework development	Develop a unified control framework based on SOC CMM, NIST CSF & NIST SP 800-53 rev.5 covering five SOC domain areas.
3	Data collection and stakeholder engagement	Share an Information Request List (IRL), and conduct interviews/workshops with SOC, IT, risk, and compliance teams to gather insights on current operations.
4	Maturity assessment	Review artifacts, evaluate internal controls, and assess SOC maturity across five domain areas, identifying gaps and improvement opportunities.
5	Reporting and roadmap	Deliver a detailed SOC maturity assessment report with observations, recommendations, and a phased implementation roadmap.

Use cases post SOC efficacy/maturity assessment



Our engagement model

We can tailor our engagement and operating model according to your specific needs.

Staff augmentation (loan staff)	Hybrid managed model	Managed services
<ul style="list-style-type: none"> Client driven Consultants engaged on contracts Client environment and client methodologies and SOPs Automation using client provided tools. 	<ul style="list-style-type: none"> Client driven, supported by KPMG in India leadership Flexible access to our professionals Client leverages KPMG in India methodologies. 	<ul style="list-style-type: none"> KPMG in India driven and supported by client (linked to SLAs) Our delivery team Our tools and accelerators used for delivery.

Why KPMG in India?

- Specialized team of SOC and cybersecurity professionals with deep expertise in SOC domains.
- Rich experience in SOC assessments across multiple industries and security frameworks.
- Assessment approach aligned with leading risk and control standards, enabling actionable insights.
- Cost-effective engagement model delivering measurable value.

Case study – large telecom and digital solutions provider

Client is a leading technology company delivering innovative telecommunications and digital services, enhancing connectivity and communication for businesses and consumers.

Engagement objective

Enable transition from existing vendor to the client while strengthening security posture through SOC maturity, ISO 27001 readiness, and governance frameworks.

Scope of work

Transition management & governance: Establish transition office, define charter, KT plan, success KPIs, and governance reporting.

SOC maturity assessment: Baseline SOC capabilities, identify gaps, and develop a roadmap (year 1 & year 2).

Infosec audit readiness: ISMS policy design, risk assessment, training, and ISO 27001 pre-certification readiness.

PMO & continuous monitoring: SLA/KPI governance, risk tracking, compliance monitoring.



Our approach

1. Designed and implemented a governance model for transition, including clear roles, responsibilities, and success metrics to enable handover.

2. Conducted review of security operations, benchmarked against industry standards, and developed a phased roadmap for maturity enhancement.

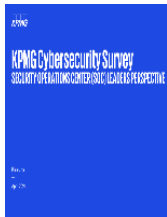
3. Built an ISO 27001-aligned ISMS framework, executed risk assessments, and delivered targeted awareness programs to embed security culture.

4. Established PMO practices for SLA tracking, compliance oversight, and risk management, supported by automation for efficiency.

Benefits to client

1. Smooth transition with less operational disruption.
2. Enhanced SOC maturity and security posture.
3. ISO 27001 readiness achieved, reducing compliance risk.
4. Improved governance through structured PMO and reporting.
5. Improved risk management through proactive identification and mitigation of transition and security risks.
6. Operational efficiency via streamlined processes and automation initiatives.
7. Enhanced compliance posture aligned with ISO 27001:2022 and industry best practices.
8. Future-ready security framework with a scalable roadmap for SOC maturity.

SOC Global Insights



KPMG Cybersecurity Survey: Security Operations Center (SOC) Leaders Perspective



Security Operation Center (SOC) Service KPMG Cybersecurity



The time to transform is now: KPMG Security Operations Center Survey 2024



Deliver value by redefining security operations with AI



SOC leaders: Adopt a Zero Trust mindset to secure external—and internal—network threats. Transformation assumes security can adapt with demand

Note: For India-specific insights, please contact KPMG in India team

KPMG in India contacts:

Nitin Shah

Partner and Head – Cyber Security and Privacy GRC

E: nitinshah@kpmg.com

Vibhav Pachori

Partner – Cyber Security and Privacy GRC

E: vibhavpachori@kpmg.com

Nakuleesh Sharma

Director – Cyber Security and Privacy GRC

E: nakuleesh@kpmg.com

kpmg.com/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.

© 2025 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only.

kpmg.com/in