Evaluate the maturity and capabilities of your Security Operations Centre

Cybersecurity has become top-of-mind for many organisations. According to PwC's 2025 Global Digital Trust Insights Survey, more than three fifths (66%) of CIOs rank cyber risks as the most critical threats their organisations plan to mitigate within the next 12 months. This highlights the importance of ensuring the **efficiency and maturity of security operations,** not only for individual organisations but also for the solutions provided by Managed Security Service Providers (MSSPs).

To achieve this, PwC's experts utilise the **SOC-CMM** (Security Operations Centre – Capability Maturity Model) **methodology**, which offers a structured **assessment of your Security Operations Centre (SOC)**.

Our team can assist you in identifying critical areas for improvement and provide tailored recommendations to help improve your operational maturity.

The SOC-CMM assessment can help:

Organisations:

- increase resistance to cyber threats
- ensure regulatory compliance (NIS2, Cybersecurity Act), best practices and international standards
- assist management in making informed decisions regarding cybersecurity investments
- increase the confidence of stakeholders, clients, and regulatory authorities in the organisation's capacity to effectively manage security threats and incidents
- assess the quality of the contracted service and identify areas for improvement

Managed Security Service Providers:

- verify and maintain a high standard of service quality
- enhance your service's market positioning
- plan service improvements
- streamline resources and boost efficiency
- build client trust

Assessment of the Security Operations Centre using the SOC-CMM methodology

The SOC-CMM model consists of 5 domains and 26 aspects, that are each evaluated using a specialised tool.

The following domains are included in the maturity assessment:

1. Business – converting business requirements into security and incident management specifications
2. People – the quantity and type of staff competencies available
3. Process – presence of all necessary processes and the evaluation of their maturity
4. Technology – capability of technology used
5. Services – capability of core services delivered by the provider

The assessment is performed by PwC's experts who have extensive experience in operational cybersecurity and are certified in the SOC-CMM methodology. Our team gathers data through workshops and interviews with key stakeholders, reviews overall and process documentation, and examines the technology in use. Subsequently, they document the evidence supporting their final conclusions and provide an expert opinion and evaluation.

This methodology allows for the measurement of SOC maturity, facilitating objective evaluations and data-driven decision-making.

PwC's team

Igor Hitrec

Senior Manager, Risk Assurance Services, PwC Croatia
SOC-CMM Certified Assessor (SOC-CA)
igor.hitrec@pwc.com

Arijan Šimek

Senior Consultant, Risk Assurance Services, PwC Croatia
SOC-CMM Certified Assessor (SOC-CA)
arijan.simek@pwc.com