Service Organization Controls 2 (SOC 2)

Effectively manage and monitor third-party risks

Overview of SOC 2 reports

Businesses are increasingly reliant on third-party suppliers to deliver business-critical services. Many of these services relate to information technology (IT), including managed IT services, software as a service (**SaaS**), and **security** as a service. These third-party services can help businesses remain competitive globally, create new market opportunities, or reduce costs while increasing quality.

However, this growing use of a complex network of third-party suppliers is fueling **concerns over IT corporate governance**, such as cyber and security threats, data quality issues, privacy laws and regulatory requirements. Each company, whether regulated or not, is ultimately responsible for the risks inherent in these engagements. It is therefore imperative that they manage and monitor these risks effectively.

Today, more than ever, organizations need to **ensure the security**, **availability**, **privacy**, **processing integrity** and **confidentiality of their data** and **underlying systems**—regardless of whether they managed are in-house or outsourced. Deloitte Azerbaijan's Information & Controls Assurance practice specializes in detecting risks that affect internal systems, business processes, projects, applications, data and third-parties with a focus on the block-chain, cloud computing and IT security sectors, as well as developing controls to address any identified risks.

The **SOC 2 reporting standard** is an **audit opinion report** on internal controls over a wide range of risk areas, including, but not limited to, organizational structure, IT, human resources, and third-party management, while focusing on the trust principles of **security, availability, processing integrity, confidentiality,** and **privacy**. As emerging technologies like cloud computing, security as a service, and block-chain have matured and new economic realities have driven organizations to boost efficiencies through outsourcing, companies need robust answers to questions about the integrity, availability and confidentiality of information managed by third-parties.

Stakeholder and regulatory requirements around internal controls are intensifying, even for companies that do not use third-parties. **A SOC 2 report can help companies address these issues and provide more assurance with regard to their service providers' internal controls to tackle any identified risks head on.**

Benefits of a SOC 2 report

A SOC 2 report follows an **extensible framework** that **enables service auditors to incorporate various industry standards** (e.g. ISO 27001, NIST, and CSA) into a unique report. SOC 2 reports are highly valued by a diverse range companies, as well as their customers.

The benefits for companies are significant, as service auditors can issue a single report instead of replying to hundreds of individual audit requests, customer questionnaires, and requests for proposals. Moreover, a SOC 2 report demonstrates management's **commitment** to building a strong internal control framework, as well as the **company's compliance** with **common control frameworks** and **robust governance over internal controls**.

By **providing a standardized format** for meeting a broad range of regulatory and industry control requirements, SOC 2 reports eliminate the need for third-party service providers and other companies to undergo multiple audits and can provide responses to several addresses. The trust criteria are directly linked to companies' core service obligations and commitments in areas such as cloud computing (e.g. infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS), block-chain, and managed IT services. These considerations cannot be sufficiently covered by a SOC 1 report, which only focuses on controls at a service organization that are relevant to user entities' internal control over financial reporting.

SOC 2 reports are also vitally important to by the **customers** of **outsourcing service providers**, as these reports reduce the amount of resources required for third-party oversight. Customers can receive independent assurance over controls operated by the service provider and obtain a comprehensive overview of the process and controls in place.

The SOC 2 report also clearly **describes the controls** a user entity must perform with respect to third-party service providers to ensure that the user entity's internal control framework is complete and addresses all relevant requirements.

Lastly, SOC 2 reports give customers insights into any deficiencies in the design of a service provider's control framework. They can then **quickly rectify these deficiencies to ensure compliance with regulations**, as well as their **own customers' requirements** and the **company's internal controls.**

Deloitte Azerbaijan's service offering

As an independent third-party service auditor, **Deloitte Azerbaijan can**:

- **Help companies prepare for SOC 2 report attestation**, including the identification of key areas necessary for compliance with SOC 2's methodological requirements, as well as other industry standards;
- **Perform control testing** in line with the applicable standard and **sign the audit opinion** accordingly**.**

As part of Deloitte's global network of member firms, Deloitte Azerbaijan has the depth and breadth of experience to deliver outstanding SOC 2 reporting services. We work closely with our clients to proactively identify **value-added business insights**, provide **suggestions for improvements throughout the engagement**, and **ensure a smooth and consistent process**.

Deloitte Azerbaijan has **developed a comprehensive** and **structured approach for SOC 2 reporting services**. Our methodology for preparing and delivering SOC 2 reports is based on a phased approach, customized to meet the specific business needs of our clients in the cloud-computing, block-chain and IT managed services sectors.

Our approach incorporates a **risk-centric focus**, while also scoping out effective methods for identifying objectives, testing controls, and executing all the tasks required for a seamless SOC 2 reporting process. We **tailor our service to your needs**, reducing the burden on you to gather the required information while helping you and your staff gain a clearer understanding of SOC 2 requirements.

We provide a carefully selected project team with in-depth industry knowledge and expertise, as well as experienced service auditor professionals. We are familiar with the **relevant frameworks, including ISO 27001**, **CSA** and **COBIT**, and **have all the required certifications**.

Contacts

Vladimir Remyga

Director
Risk Advisory
vremyga@deloitte.com
Tel.: +994 (012) 404 1210
Mob.: +994 51206 0123; +7 (700) 714 5505

Vladimir is a Director in the Risk Advisory department. He leads Deloitte's digital and cyber security services in the Caspian and Caucasus regions. Vladimir has over twenty years' experience in IT and cyber security and serves a diverse range of clients across the CIS region. He specializes in digital and cyber risk management, IT cost optimization and digital-driven transformations.
He joined Deloitte in 2019 and shares his time between Azerbaijan, Kazakhstan, Georgia and Uzbekistan. Prior to joining Deloitte, Vladimir was based in Almaty, Kazakhstan where he was IT Advisory Director at a global consultancy firm.
He received his MBA in Entrepreneurship from Moscow International Business School (MIRBIS).
Vladimir also holds an honors degree in Information Security and Protection from Kazakh National Technical University.
Vladimir is a certified professional in CISA, CISSP, CRISC, PRINCE 2 and ISO 27001 LA.

Gamar Gadimli

Assistant Manager
Risk Advisory
ggadimli@deloitte.az
Tel: +994 (012) 404 12 10 (4323)

Gamar is an Assistant Manager at Deloitte Azerbaijan.
Gamar has more than six years' experience in the Risk Advisory department. She has served companies from sectors as varied as finance, telecoms, oil & gas, logistics, aviation and hospitality.
Gamar is responsible for operational risk services, including internal audit, service organization audit, and operational risk management transformation projects. She also leads the IT Audit practice and helps clients manage their IT risks to drive efficiency and reduce costs.
She has headed projects to test and develop IT audit, internal control, control assurance processes for a number of companies. Gamar also manages efficiency assessment, process development and organizational restructuring assignments.