prosource™

Cloud Security Assessment Checklist

Scope Definition	
□	Ensure a thorough understanding of the business context to identify critical services and assets accurately. Consider the potential consequences of compromised assets to prioritize them appropriately.
□	Engage with stakeholders from different departments to gather insights on the sensitivity and importance of data and services, ensuring all critical areas are included in the scope.
Data Collection	
□	Maintain an inventory of all configurations and security settings to streamline the data collection process.
□	Focus on the accuracy and comprehensiveness of collected data, including user access levels, encryption standards, and existing security protocols, to ensure a solid foundation for further analysis.
Vulnerability Identification	
□	Stay updated on the latest vulnerability scanning tools and techniques to effectively detect new and evolving threats.
□	Prioritize a methodical approach to testing, ensuring each component within the defined scope is scrutinized for vulnerabilities.
Risk Assessment	
□	Develop a clear understanding of your organization's risk tolerance to effectively categorize and prioritize vulnerabilities based on potential business impact.
□	Incorporate industry benchmarks and historical data to assess the likelihood of vulnerability exploitation more accurately.
Recommendations	
□	Provide actionable and practical recommendations tailored to the specific architecture and operational practices of your organization.
□	Focus on both immediate fixes for high-risk vulnerabilities and long-term security enhancements to prevent future threats.
Report Generation	
□	Ensure clarity and detail in reporting to make the findings accessible and actionable for all stakeholders, including technical and non-technical audiences.
□	Highlight critical vulnerabilities and their potential impacts clearly, and provide a prioritized list of recommendations.
Follow-Up	
□	Establish metrics and benchmarks to measure the effectiveness of implemented security measures.
□	Schedule regular follow-ups and reviews to adapt to new threats and changes in the organization's cloud environment, ensuring ongoing protection and compliance.