

Cloud Security Assessment

EY Ukraine Digital



The better the question. The better the answer. The better the world works.



Shape the future
with confidence

Client brochure

Cloud Security Assessment is focused on evaluating cloud's main functions

How is your cloud built?

- Develop and implement cloud security controls framework and security reference architecture customized to client business, regulatory and client control environment needs.
- Identify, develop and build cloud security reference architecture for network, platform and application layers of the cloud environments.
- Focus on preventive and configuration controls.
- "Path to production" cloud security checklists.

How is your cloud operated and monitored?

- Manage vulnerabilities, threats and incidents in the cloud and hybrid infrastructure and deployments using cloud-native and third-party tools.
- Cloud security monitoring benchmarks.
- Feedback loop for consistently and methodically integrating relevant security mechanisms into cloud development.
- Focus on run-time workload protection tools.



Our approach

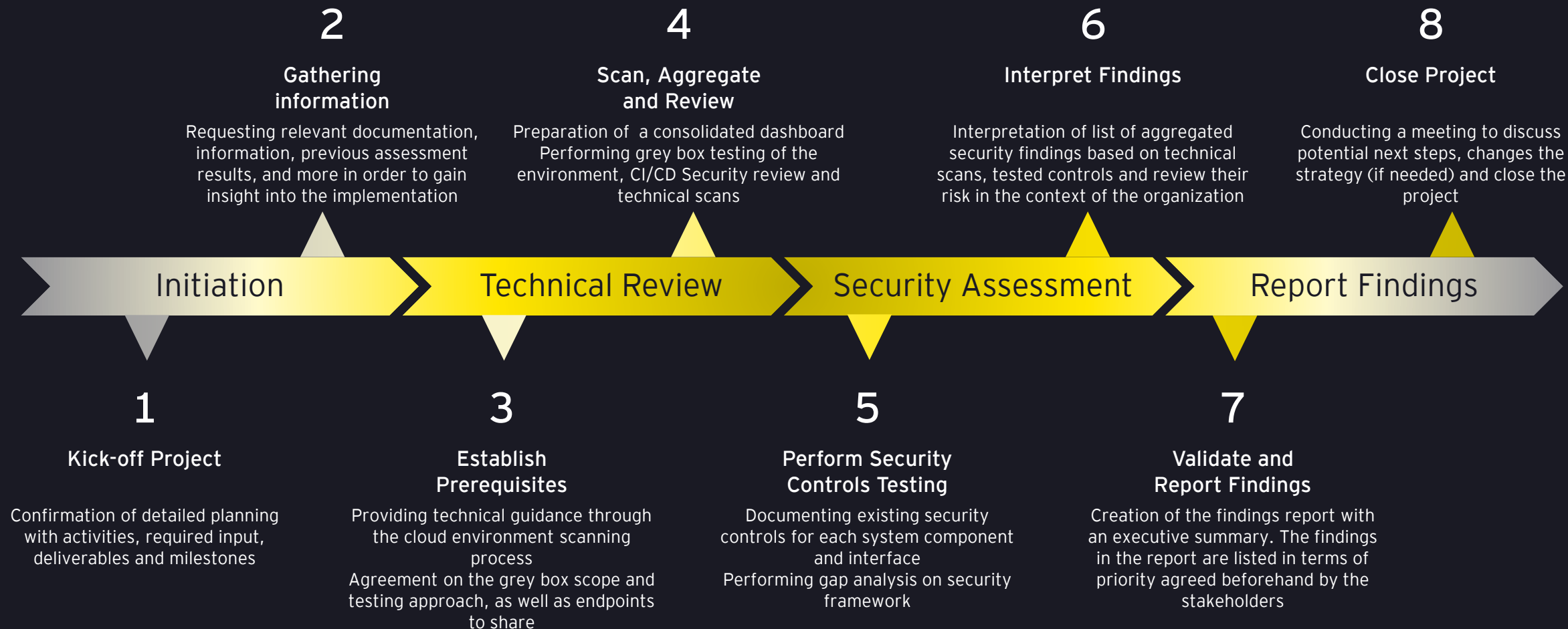
Cloud Security Assessment is a comprehensive solution that tests and analyses organization's cloud infrastructure and provide actionable recommendations.

This Solution helps to secure the whole cloud environment, create security controls, configuration checks, monitoring, and reporting and start automated enforcement.



Cloud Security Assessment Roadmap

EY's differentiated approach will utilize cloud security controls and processes framework to conduct a cloud security assessment of current cloud architecture, information security controls, cloud use cases, and applicable standards to assess the risk of cloud usage.



Cloud Security Intelligence Platform overview

Cloud Security Intelligence Platform (CSI) is used during the Technical Review Phase*

CSI Overview

- CSI scans cloud environments and outputs findings based on EY's Findings Database:
 - **Cloud environment:**
 - Possibility to scan multiple Azure subscriptions, AWS accounts or GCP projects or the entire tenant
 - Meta-data is gathered to detect misconfigurations, no actual data is ever read or stored
 - **Data Storage:**
 - In a private Azure storage account (only accessible by the person in charge of the assessment)
 - Raw output of the scanning tools
 - Final result: Aggregation of the raw output from the scanning tools.
 - Retention period is limited to two weeks after the assessment to address any Client concerns for which EY may rely on the raw output
 - **Data Processing:**
 - The raw data is gathered by means of automated tooling that interacts with Client's cloud environment
 - The raw data is processed and matched against our EY Findings Database, enhanced by EY's custom risk and business impacts & remediations
 - For each scan, the collected data is processed on a new virtual machine. There is no data persistence between scans and it is not possible to extract the data directly from the agent
 - **Frameworks:**
 - PCI-DSS
 - CIS (multiple versions)
 - NIST
 - Microsoft Best Practices

CSI Flow Overview



* Usage of CSI scanning is performed only based on agreement with the client. Another tools can be used or technical review step can be skipped.

For cloud service providers, we can perform a security assessment based on the C5 (Cloud Computing Compliance Criteria Catalogue) standard

For cloud service providers, we offer a SOC 2+ report or an ISAE 3000 report with C5 controls



EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2025 EY Ukraine Digital.
All Rights Reserved.

[This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global EY organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

ey.com