Google Cloud

Course 2 glossary

Terms and definitions from Course 2

A

Assured Workloads: Tool that manages security and compliance of Google Cloud workloads

B

Boolean constraints: Constraints that are either enforced or not enforced for a resource; govern a specific behavior

C

Cloud audit: An assessment of the cloud environment that is usually conducted by a third party

Cloud organizational policy: A set of restrictions or constraints on a specific cloud service, or list of services

Cloud Protection +: A specialized insurance policy developed by Google in collaboration with insurance carriers, and available through the Risk Protection Plan

Cloud security controls: Controls that safeguard cloud environments from threats, and minimize the effects of harmful attacks

Cloud security posture management (CSPM): The process of monitoring and configuring cloud assets for security and compliance with best practices, regulations, and organization policy

Compensating controls: Measures that make other controls more effective

Compliance: The process of adhering to internal and external standards, and government regulations

Compliance lifecycle: The process for ensuring compliance objectives are met and maintained to support the business goals

Constraint: A restriction against a Google Cloud service, or a list of services

Control inheritance: The process of using controls or compliance certifications and audits that are already provided by a cloud service provider

Cyber insurance: A type of policy that covers businesses against financial losses resulting from cyber incidents

H

Hierarchy: A system that organizes or ranks things, usually by power or importance

I

Infrastructure as code (IaC): The practice of automating and managing infrastructure using reusable scripts

L

Likelihood: The probability that a vulnerability will be exploited by a threat actor, and includes the extent of the impact of the threat

List constraints: Rules that allow or disallow a set of values

M

MITRE: A not-for-profit organization that conducts research to support government agencies

Multicloud: A strategy of using more than one cloud service provider

Multicloud cloud security posture management (CSPM): The process of assessing the security of assets throughout a multicloud environment

N

National Vulnerability Database (NVD): A publicly accessible repository of data about known system and software vulnerabilities

Non-compliance: The failure to follow standards and regulations that are set by internal standards and policy, or external laws and regulations

O

OWASP® Top Ten: A regularly updated report of critical security risks for web applications

P

Policy as code (PaC): The use of code to define, manage, and automate policies, rules, and conditions using a high-level programming language

R

Risk: The measure of how much a threat impacts the confidentiality, integrity, and availability of an asset

Risk management framework: A set of practices, processes, and technologies that enable an organization to identify, assess, analyze, and manage risk within an organization

Risk Protection Program: A solution that provides insurance carriers with accurate information about an organization's level of risk

Role binding reports: Sets of one or more members and identities, known as principals, who have a permission or role granted by the cloud security team

S

Security Command Center Google Cloud's centralized vulnerability and threat reporting service

Security control: A safeguard designed to reduce specific security risks

Security domain: A collection of tightly coupled security practices that address a specific security discipline

Shared fate model: An approach that emphasizes the cloud service provider's (CSP's) involvement in the customer's entire security journey, and offers resources to securely manage their environment at each stage

T

Threat: Any situation or circumstance that can negatively impact assets

Threat modeling: The process of identifying assets, their vulnerabilities, and how each is exposed to threats

U

Underwriting: An insurer's process of pricing an insurance policy

V

Vulnerabilities: Weaknesses that can be exploited by threat actors

W

Web Security Scanner: Detects vulnerabilities in App Engine, GKE, and Compute Engine applications