



! Try again once you are ready
TO PASS 66% or higher

Try again

GRADE
38.88%

Module Quiz

LATEST SUBMISSION GRADE

38.88%

1. Which ONE of the following statements is TRUE concerning Google's built-in security measures?

0 / 1 point

- ☒ An organization's on-premises resources are not allowed to connect to GCP in order to lower the risk of DDoS attacks.
- ☐ To guard against phishing attacks, all Google employee accounts require the use of U2F compatible security keys.
- ☐ Only Google managed encryption keys are allowed to be used within Google Cloud Platform.
- ☐ Customers always have the option to configure their instances to encrypt all of their data while it is "at rest" within GCP.

! Incorrect

You may wish to review Lesson 1 before attempting this quiz again.

2. Which TWO of the following statements are TRUE regarding regulatory compliance on Google Cloud Platform?

0.5 / 1 point

- ☒ Contacting your regulatory compliance certification agency is the only way to find out whether Google currently supports that particular standard.



This should not be selected

You may wish to review Lesson 1 before attempting this quiz again.

- ☒ Google has no plans at this time to expand its already-extensive portfolio of regulatory compliance certifications.



This should not be selected

You may wish to review Lesson 1 before attempting this quiz again.

- ☒ Google's Cloud products regularly undergo independent verification of security, privacy, and compliance controls.



Correct

Correct! Google works to achieve certifications against global standards so we can earn your trust.

- ☒ Proper configuration of encryption and firewalls is not the only requirement for achieving regulatory compliance.



Correct

Correct! You also need data protection that is in compliance with the regulatory standards you wish to meet.

3. Which TWO of the following statements are TRUE regarding Google's ability to protect its customers from DoS attacks?

0.667 / 1 point


- ☒ A single Google data center has many times the bandwidth of even a large DoS attack, enabling it to simply absorb the extra load.



Correct

Correct! A large attack can be around 1 Tb per second, but a typical Google Data Center has a bandwidth capacity of around 1300 Tb per second.

- ☒ Application-aware defense is not currently supported on GCP, although support for this is planned in the very near future.

 **This should not be selected**

You may wish to review Lesson 2 before attempting this quiz again.

- ☒ Google Front End can detect when an attack is taking place and can drop or throttle traffic associated with that attack.

 **Correct**

Correct! Further, when you use Google Load Balancers, this protection kicks in automatically, without the need for further configuration.