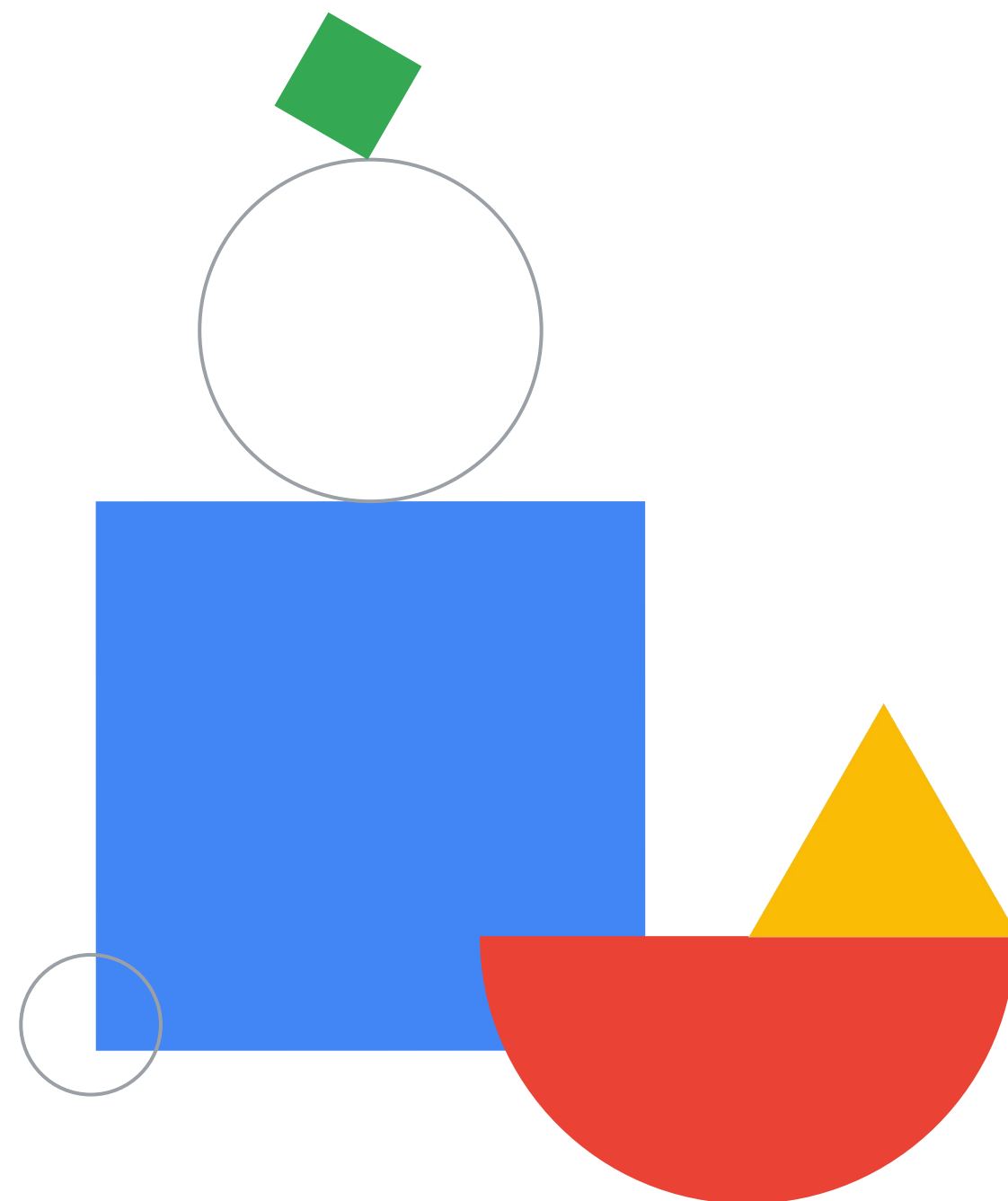


Preparing for Your Professional Cloud Security Engineer Journey

Introduction

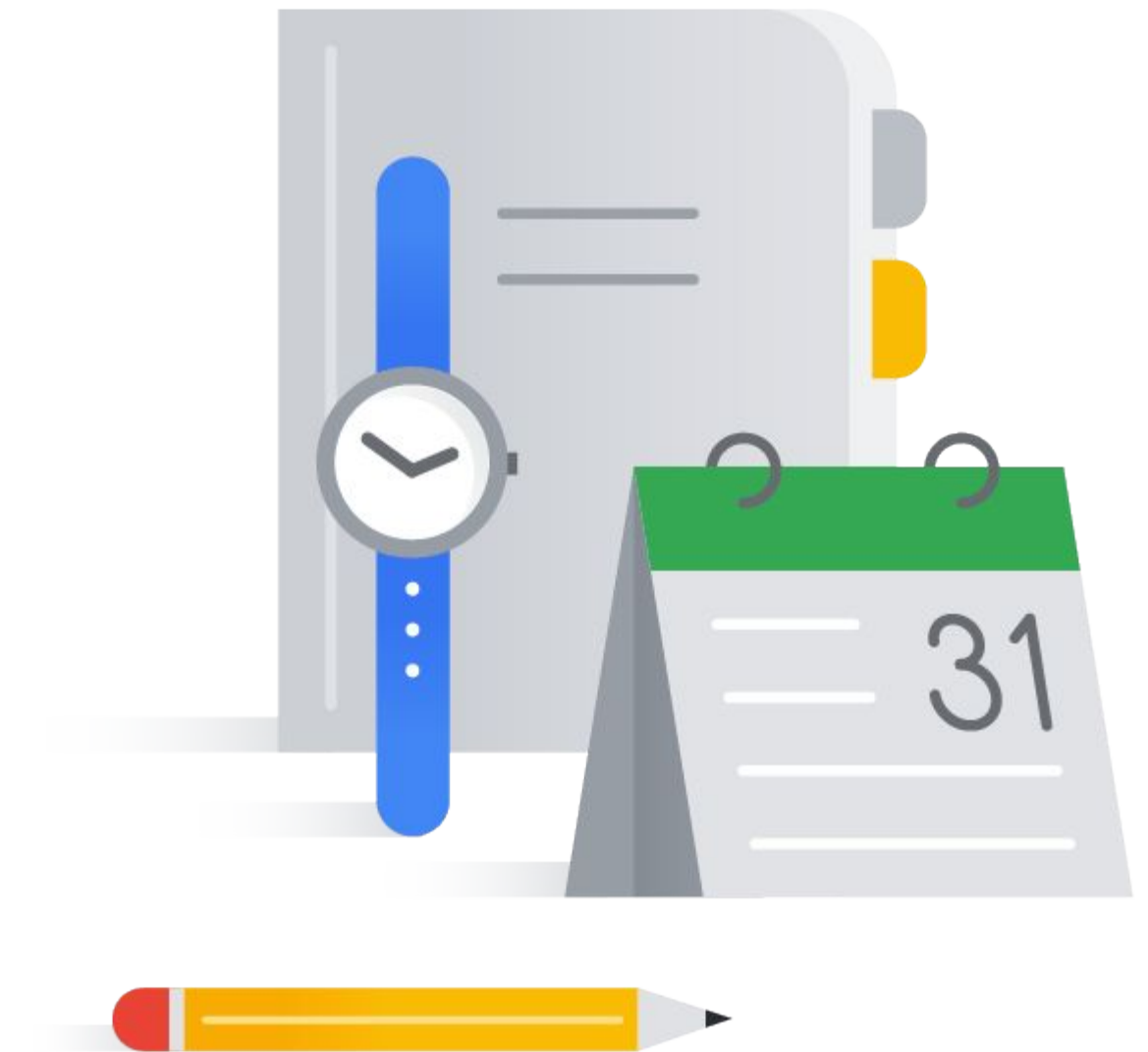


**Who am I and
what's my role here?**



Course agenda

- | | |
|---|--|
| 0 | Introduction |
| 1 | Configuring Access Within a Cloud Solution Environment |
| 2 | Configuring Network Security |
| 3 | Ensuring Data Protection |
| 4 | Managing Operations in a Cloud Solution Environment |
| 5 | Ensuring Compliance |
| 6 | Your Next Steps |



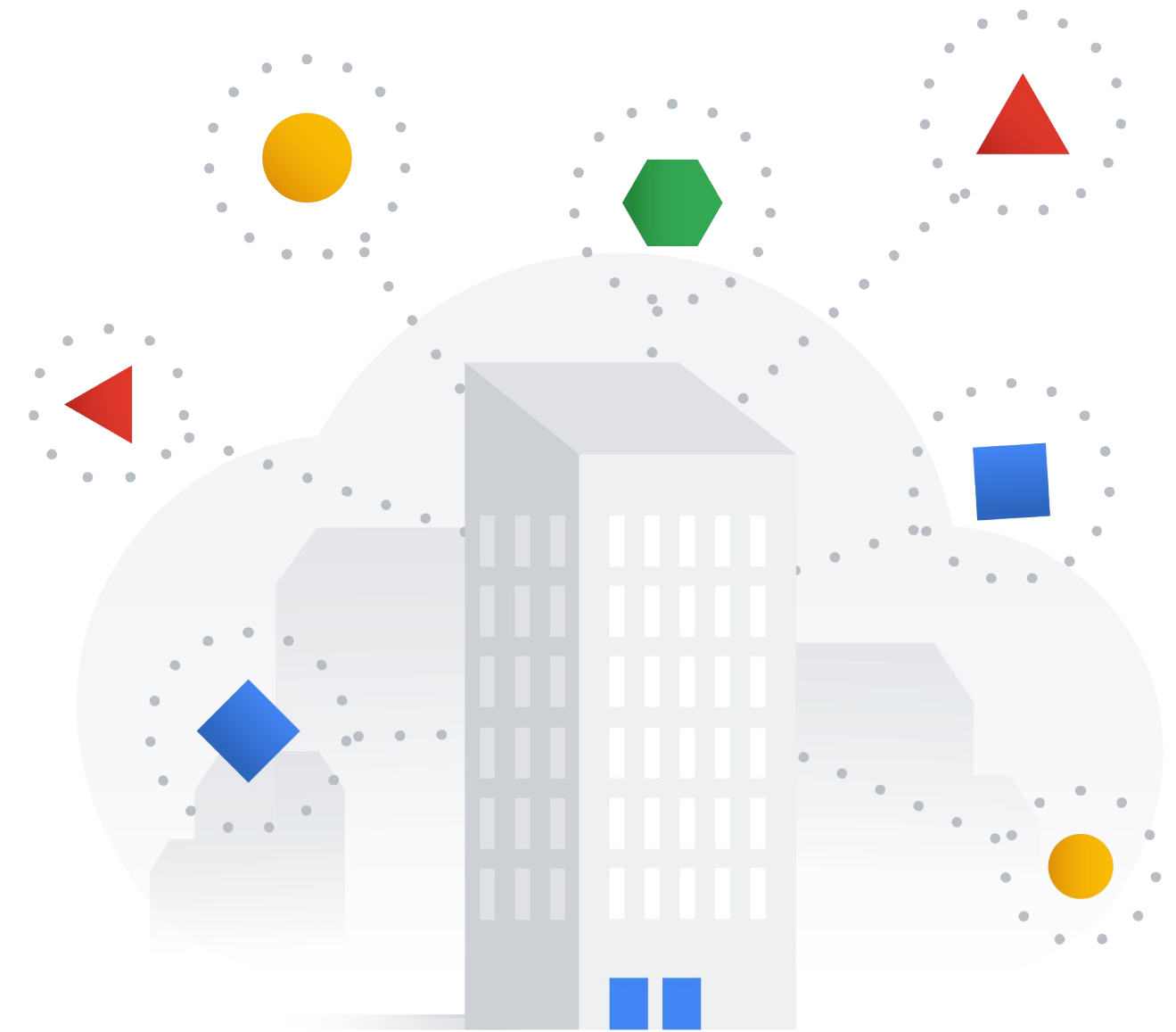


Module agenda

- 01 What is the role of a Professional Cloud Security Engineer?
- 02 Resources to support your certification journey
- 03 Creating your study plan

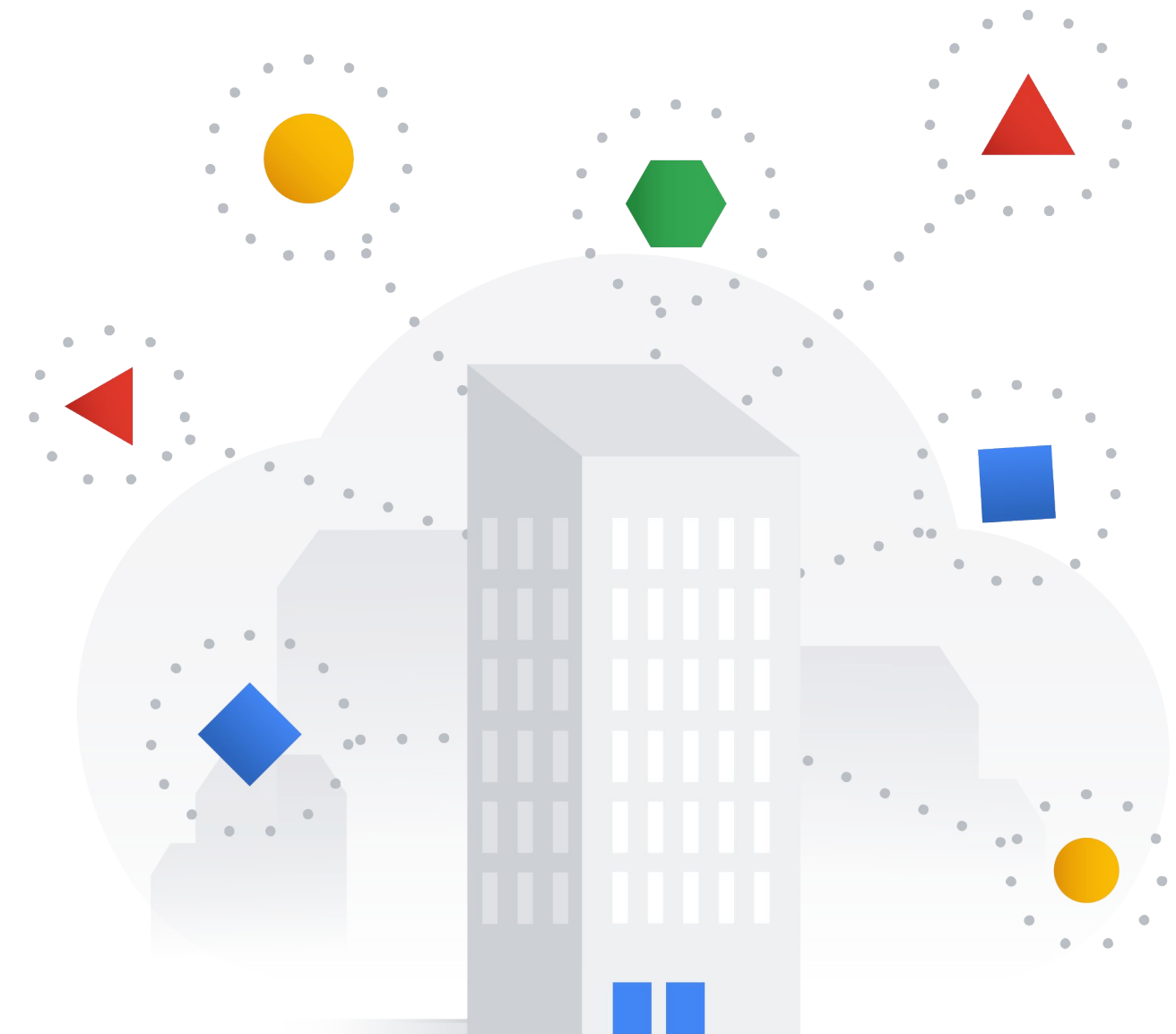


What is the role of a Professional Cloud Security Engineer?



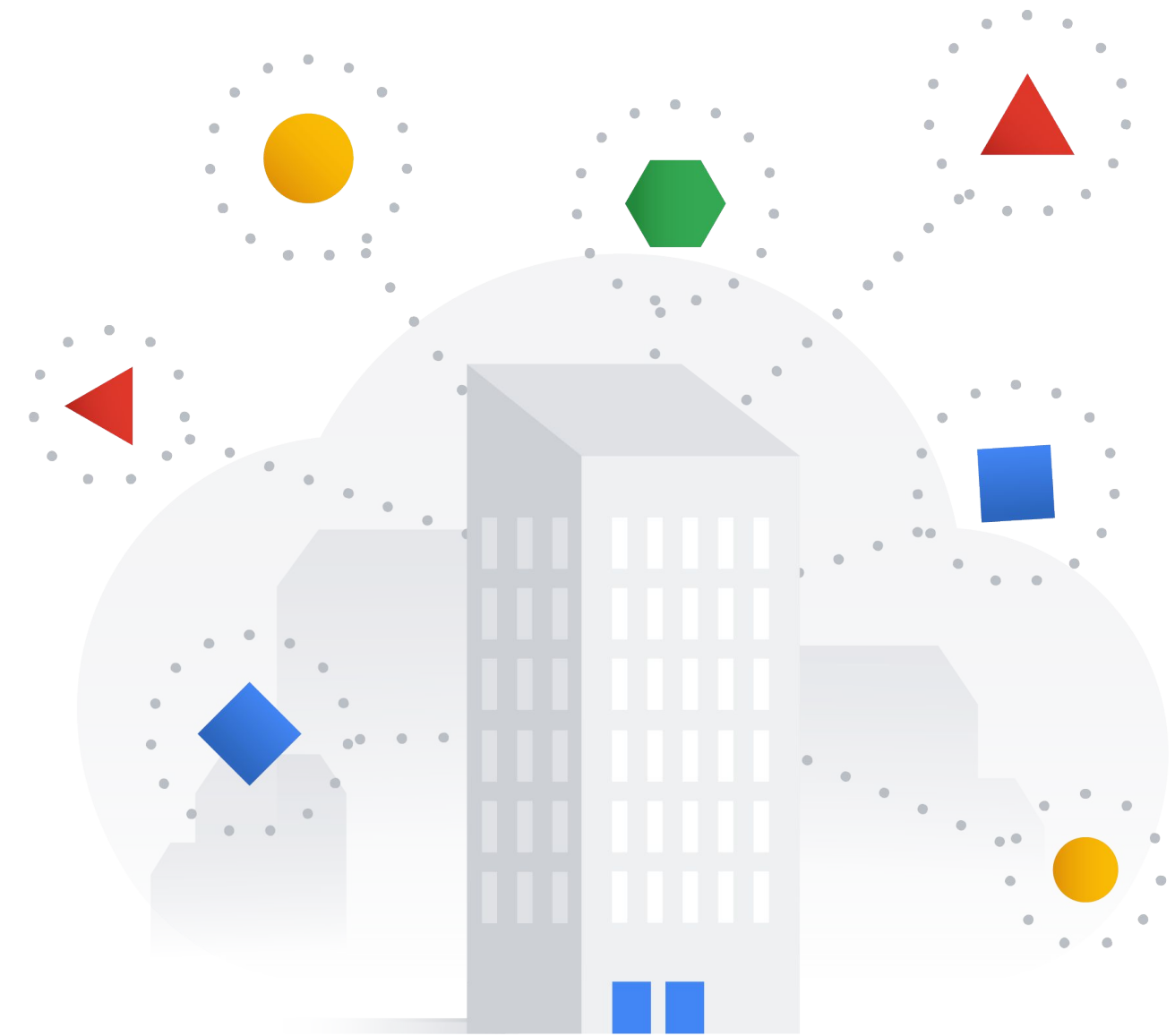
What is the role of a Professional Cloud Security Engineer?

- Enables organizations to design and implement secure workloads and infrastructure on Google Cloud
- Designs, develops, and manages a secure infrastructure by leveraging Google Cloud security technologies

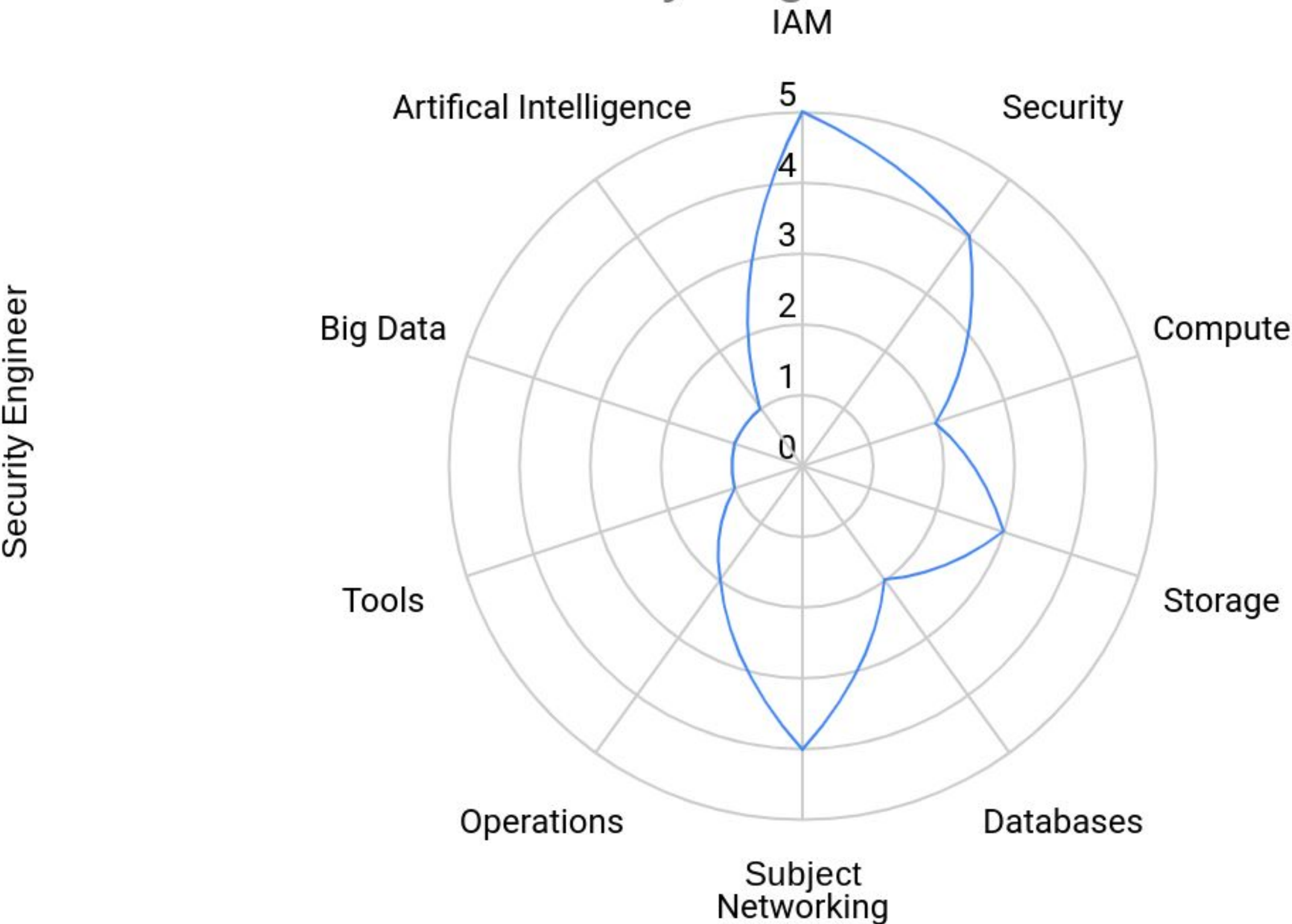


What is the role of a Professional Cloud Security Engineer?

- Should be proficient in:
 - Identity and access management
 - Defining organizational structure and policies
 - Using Google Cloud technologies to provide data protection
 - Configuring network security defenses
 - Collecting and analyzing Google Cloud logs
 - Managing incident responses
 - Applying dynamic regulatory considerations
- For more information, visit the [Professional Cloud Security Engineer certification](#) page



Professional Cloud Security Engineer



PCSE Exam High-level Overview

- How to position PCA? One of [9 professional level exams](#) (+ [CDL](#) & [Associate Cloud Engineer](#))
- 80h-150h+ to complete. Consistency is the key! 2-3 hours a day, starting from now...
- Exam structure:
 - 50 questions / 2h for the exam. **Pro tip: Handle the easier questions first (aim at ~1.5 min per question), mark the rest for review. Also, don't leave any questions unanswered (no negative points).**
 - Multiple-choice theoretical questions, but asking about “real-world” challenges. Most with a single correct answer, some with more (you will know how many). Get a feeling by doing a [sample test](#).
 - In a lot of cases, you will need to choose BEST answer from 2-4 which are technically correct.
 - NO labs, NO hands-on exercises (but essential when preparing!), NO case-studies on the exam.
 - English language only (no additional time for non-native speakers).
- When you submit the exam, you'll only see PASS / FAIL.
 - You will NOT be presented with any details of accuracy / areas to improve etc.
 - It's not clear what is the percentage needed to pass (aim at 85+% accuracy for practise questions).
- Can be taken online or at a testing center. Sign up [here](#).
- Certificate is valid for 2 years.
- If you fail, retake policy is: 14 days / 60 days / 1 year (separate voucher needed for each attempt)
- [20-min video on how to prep for PCSE and PCNE exam](#)

Exam question - example

Notice the business context

A Cloud Development team needs to use service accounts extensively in their local environment. You need to provide the team with the keys for these service accounts. You want to follow Google-recommended practices.

What should you do?

- A. Implement a daily key rotation process that generates a new key and commits it to the source code repository every day.
- B. Implement a daily key rotation process, and provide developers with a Cloud Storage bucket from which they can download the new key every day.
- C. Create a Google Group with all developers. Assign the group the IAM role of Service Account User, and have developers generate and download their own keys.
- D. Create a Google Group with all developers. Assign the group the IAM role of Service Account Admin, and have developers generate and download their own keys.

Sample quiz



Understand the scope of the exam based on the Professional Cloud Security Engineer Exam Guide.

cloud.google.com/certification/guides/cloud-security-engineer



Pro tip: Make notes while you learn!!!

- Choose your favourite tool that handles text **and images**.
- Copy & paste from GCP documentation / course transcripts
- Copy & paste important slides / images / decision trees / tables
- Use colours / bold
- Paste difficult quiz questions from quizzes etc with explanations / links to solutions
- Remember about 2-year validity of GCP certificates -> notes will most probably be very useful next time.
- **Switch between resources if you get bored.**

Custom roles

<https://cloud.google.com/iam/docs/creating-custom-roles>

Use the [gcloud iam list-testable-permissions](#) command to get a list of permissions that are available for custom roles in a specific project or organization. The response lists the permissions that you can use in custom roles for that project or organization.

To list permissions that are available in custom roles for a project or organization, run this command:

```
gcloud iam list-testable-permissions full-resource-name\  
--filter="customRolesSupportLevel!=NOT_SUPPORTED"
```

You can create a custom role at the project or organization level. = NOT ON FOLDER LEVEL!!

To view the role metadata, use one of the methods below:

```
gcloud iam roles describe role-id
```




Example:

```
gcloud iam roles describe roles/iam.roleViewer
```

```
description: Read access to all custom roles in the project.  
etag: AA==  
includedPermissions:  
- iam.roles.get
```


Pro tip no.2: be curious!

[← Create Instance Group](#)

-  **New managed instance group (stateless)**
Automatically manage groups of VMs that do stateless serving and batch processing.
 -  **New managed instance group (stateful)**
Automatically manage groups of VMs that have persistent data or configurations (such as databases or legacy applications).
 -  **New unmanaged instance group**
Manually manage groups of load balancing VMs.

☐ Single zone

☒ Multiple zones

Region * us-central1 (Iowa)

Zones
us-central1-c, us-central1-f, and us-central1-b

Target distribution shape

Even

Distribute managed instances evenly across zones

Balanced

Distribute managed instances as evenly as possible across zones given availability of resources in each zone


Any


Deploy managed instances to one or multiple zones based on availability of resources and reservations in each zone

Use autoscaling to automatically add and remove instances to the group for periods of high and low load. [Learn more](#)

Autoscaling mode

On: add and remove instances to the group

Minimum number of instances * 

Maximum number of instances * 

To maximize availability, the minimum number of instances should be at least equal to the number of zones. Additional instances will be placed in different zones.

Distributing instances using regional managed instance groups

Pro tip no.3: use GCP Free Trial 300USD (*) and Free Tier

It will help you be curious :)

- **90-day, \$300 Free Trial:** New Google Cloud and Google Maps Platform users can take advantage of a 90-day trial period that includes \$300 in free Cloud Billing credits to explore and evaluate Google Cloud and Google Maps Platform products and services. You can use these credits toward one or a combination of products.

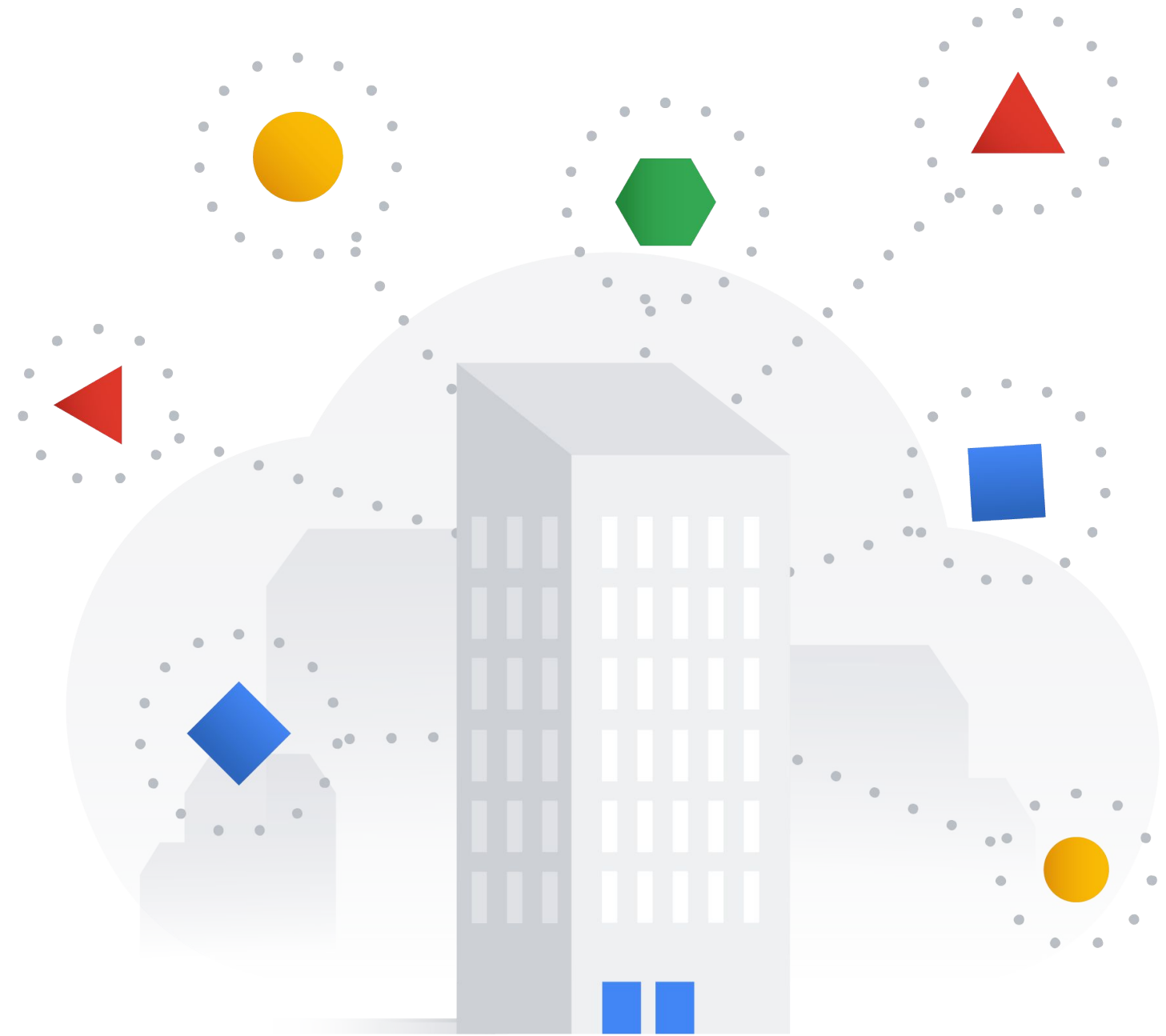
<https://cloud.google.com/free>

Thanks for signing up. Your free trial includes \$300 in credit to spend over the next 90 days. If you run out of credit, don't worry — you won't be billed unless you [turn on automatic billing](#).

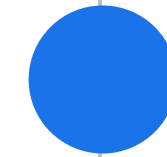
GOT IT

* To complete your Free Trial signup, you must provide a [credit card or other payment method](#) to set up a Cloud Billing account and verify your identity. Don't worry, setting up a Cloud Billing account does not enable us to charge you. You are not charged unless you explicitly enable billing by upgrading your Cloud Billing account to a paid account.

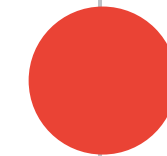
Secure Cymbal Bank's cloud environment



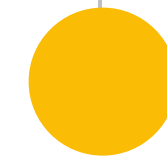
Why become Google certified?



Gain industry recognition!

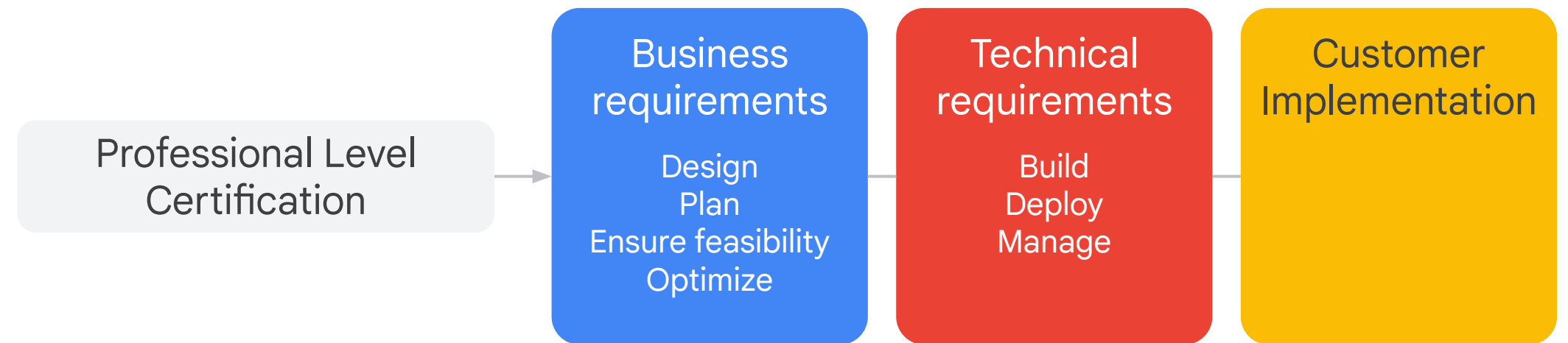


Validate your technical expertise!

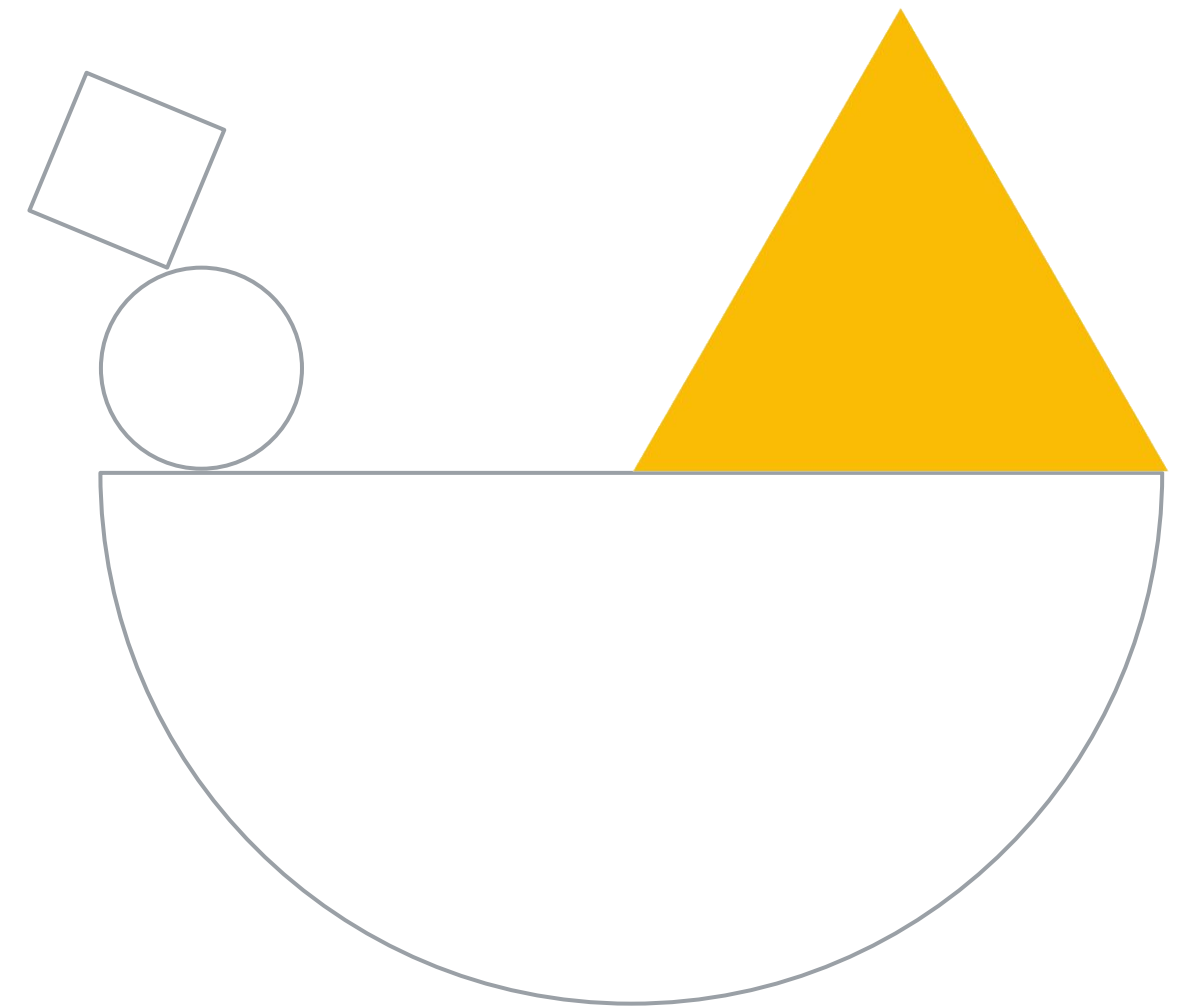


Take your career to the next level!

What is a Professional certification?



Resources to support your certification journey





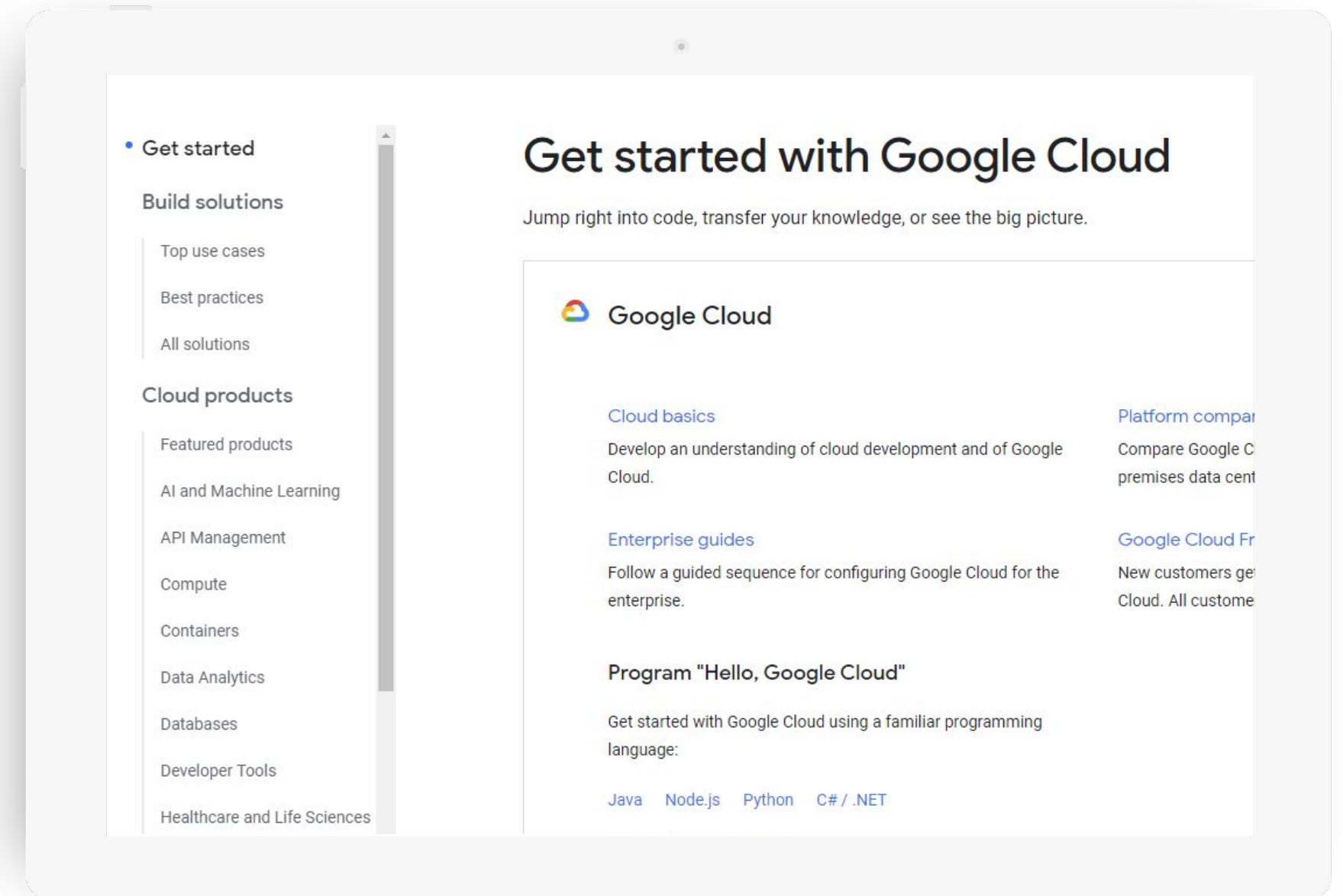
Digitally Transforming

A nationally-recognized American retail bank founded in 1920 and acquired by Cymbal in 1975.

Product Documentation

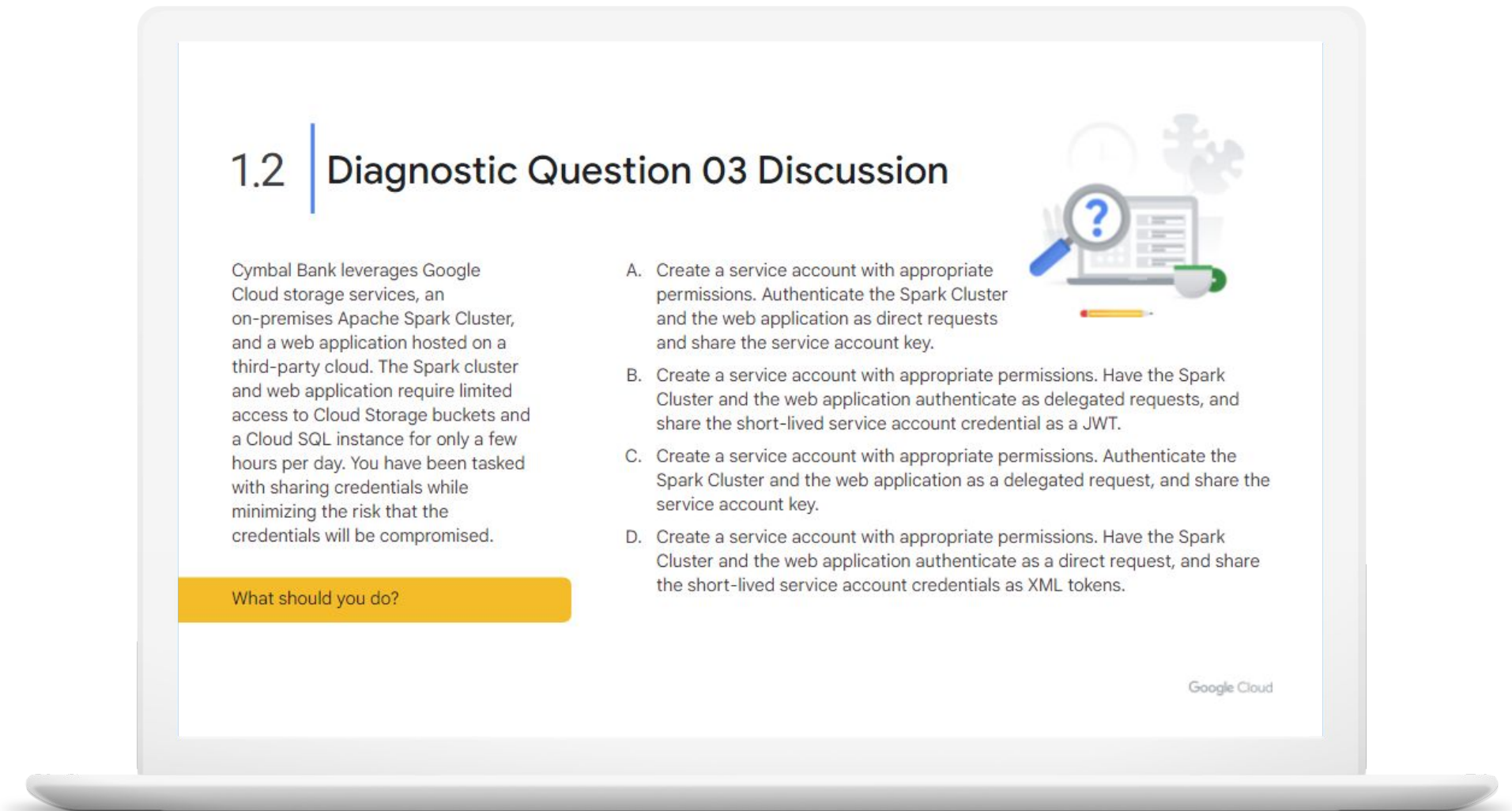
Google supplies official public documentation for its products and services.

cloud.google.com/docs



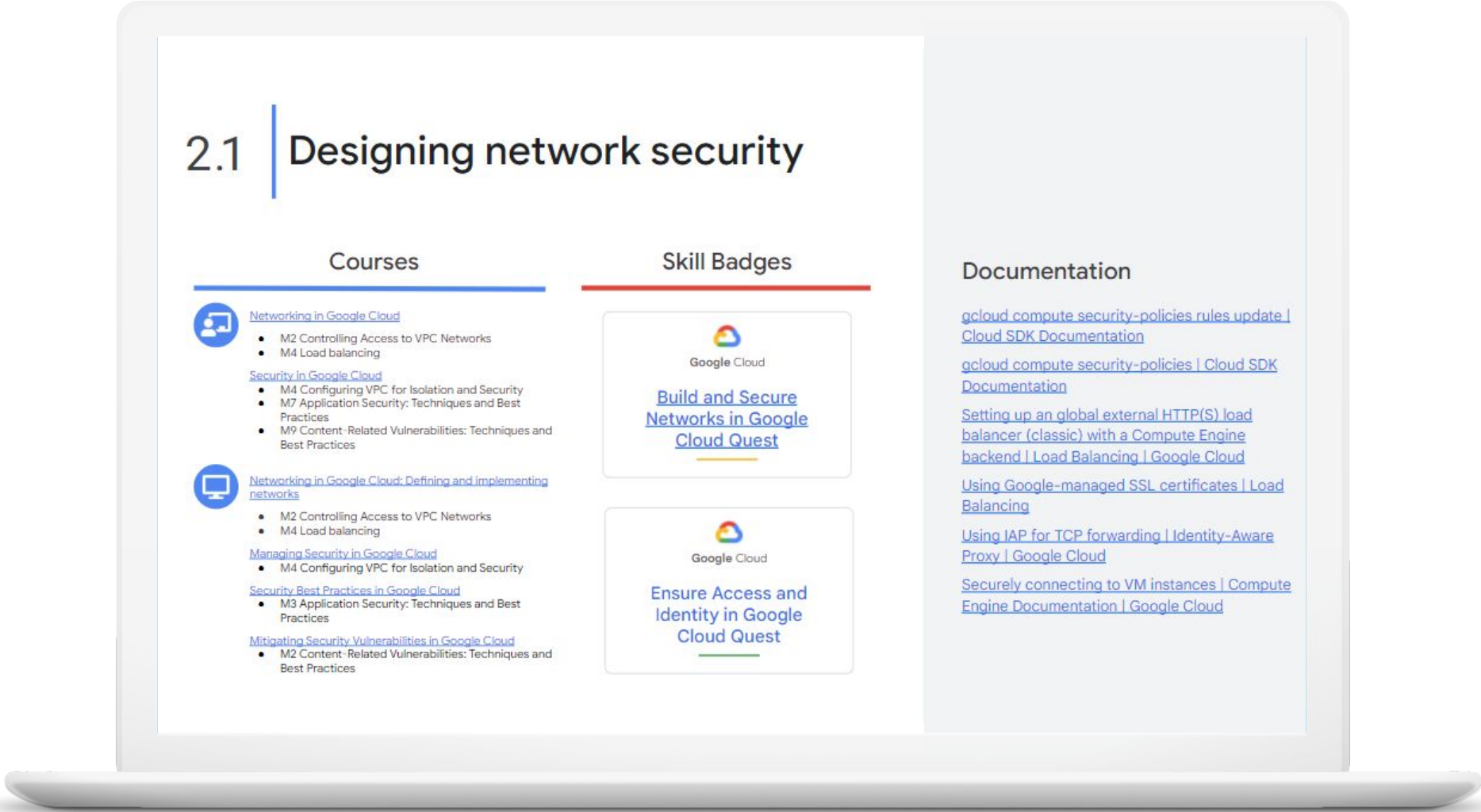
Diagnostic questions:

Identify areas you need to study and resources to support you



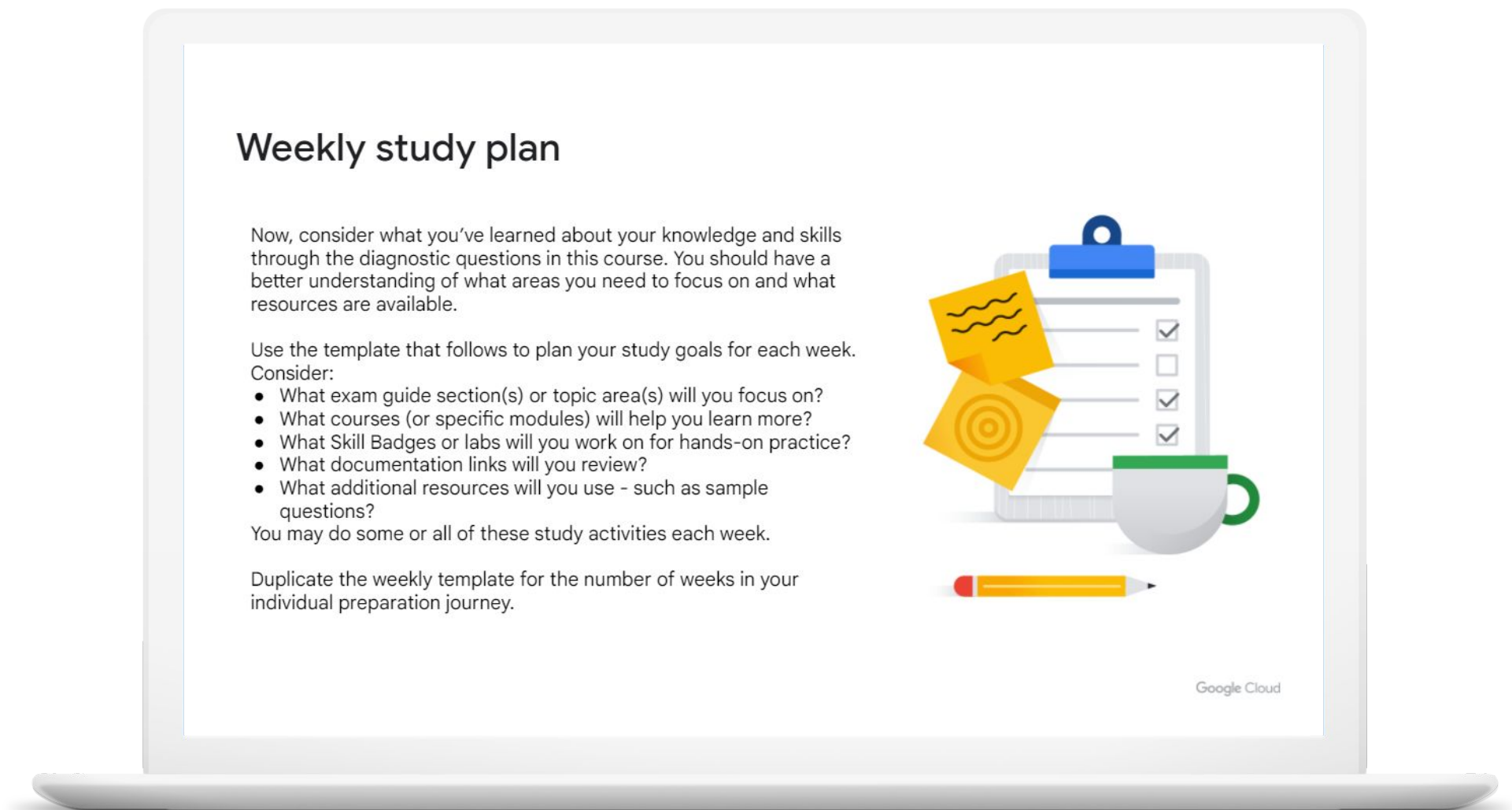
Locate resources:

Take notes in your
workbook on the
resources and
documentation to fill
your gaps



Use the workbook:

Plan your study for
each week in the journey



See what others think...

Published	Title/Link	Author
2021/10	My review on the PCSE Beta Exam	Antoni Tzavelas
2020/02	BeyondProd: A new approach to cloud-native security	Google
2019/11	Exam Study Guide	Mark Johnson
2019/11	Google Cloud Security Engineer Exam Notes	Travis Webb
2019/08	How to pass the Google Professional Cloud Security Engineer certification	Ivam Luz
2019/08	Google Cloud Security Exam Experience: RTFQ twice	Jaroslav Pantsjoha
2019/07	Exam Prep Sheet	Ammett Williams
2019/06	How to fail and then pass the Security Engineer Exam	Ammett Williams
2019/05	Google Professional Cloud Security Engineer Certification	John Hanley
2019/03	Google Professional Cloud Security Engineer—Beta exam review	Rakesh Sharma
2019/02	Notes from my beta Google Cloud Professional Security Engineer Certification Exam	Sathish VJ
2019/02	Google Professional Cloud Security Engineer Beta Exam walkthrough	Dmitri Lerko
2019/02	Google Cloud Professional Security Engineer Exam Guide	Darpan Shah
2018/03	Google Cloud Security Whitepapers	Google
	Path to Professional Security Engineer	Google

[LINK](#)

Additional resources - quizzes

Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership. 1 point

What should your team do to meet these requirements?

- ☐ Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.
- ☐ Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.
- ☐ Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.
- ☐ Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

- Aim: validate **technical** knowledge (no business context)
- NOT as complex as questions on the exam

Additional resources - GCP cheat sheet

Developer cheat sheet

Map view

List view

Get the poster on GitHub

Architecture

 Cloud IDS	 Cloud Load Balancing	 Cloud VPN	 Media CDN	 Partner Interconnect	<div>Identity and Security</div> <div>Policy and compliance tools</div>			 Container Analysis	 Cloud HSM	 Security Key Enforcement
 Direct Peering	 Network Intelligence Center	 Network Telemetry	 Private Service Connect	 Access Context Manager				 Chronicle	 Cloud Identity-Aware Proxy	 VPC Service Controls
 Traffic Director	 Transcoder API	 VPC Service Controls	 Assured Workloads	 Access Transparency				 Cloud Data Loss Prevention	 Identity Platform	 Web Security Scanner
 Cloud Billing API	 Security Command Center	 Confidential Computing	 Cloud Audit Logs	 Certificate Authority Service				 BeyondCorp Enterprise	 Binary Authorization	 Cloud Asset Inventory
 Cloud APIs	 Cloud Billing	 Risk Manager	 Event Threat Detection	 Cloud Identity	 Cloud EKM	 Cloud IAM	 Context-aware Access	 Resource Manager	 reCAPTCHA Enterprise	 Pub/Sub

[GCP Services cheat sheet](#)

Additional resources - GCP Service Summary:

- VERY subjective, NOT a Google-owned or recommended.
- Should be treated as supplemental study materials; NOT an exhaustive list or requirements.
- If it helps -> use it. If it looks scary to you -> don't 😊

		Professional Cloud Security Engineer (PCSE)		
0: not covered on the exam at all				0: none
1: basics (high-level functionality and use-cases)				1: basics
2: medium (1 + prerequisites, limitations, common IAM roles, ability to integrate with other services, most common architectures)				2: medium
3: advanced (2 + being able to deploy, troubleshoot and manage)				3: advanced
4: expert (3 + know every detail about the service in complex configurations - huge scale, HA, DR etc)				4: expert
		Recommended minimum knowledge level for PCA	My knowledge level (self-assessment)	
Security and Identity	Binary Authorization	2: medium	0: none	
	Cloud Asset Inventory	2: medium	0: none	
	Cloud Data Loss Prevention	3: advanced	0: none	
	Cloud Key Management Service	3: advanced	0: none	
	Cloud Security Command Center	2: medium	0: none	
	VPC Service Controls	3: advanced	0: none	
	Web Security Scanner	2: medium	0: none	
	Cloud EKM	2: medium	0: none	
	Cloud HSM	2: medium	0: none	
	Shielded VMs	1: basics	0: none	
	Confidential Computing	1: basics	0: none	
	Service Accounts	3: advanced	0: none	
	Titan Security Key	1: basics	0: none	
	Access Transparency	2: medium	0: none	
	Chronicle	1: basics	0: none	
	BeyondCorp / BeyondProd model	2: medium	0: none	
	Log export to SaaS			
PCA		PCSE		

LINK

Cloud Skills Boost Demo

Let's start on your
**Professional Cloud
Security Engineer journey.**

