
Hello Lori, Pasting below what I got from the CI. I think he had something very pressing happen, as I have the same one on a separate course and he has not replied even though I have emailed him a few times. Again, I just used what he recommended for External APIs on the Internal API as well:

Format the sections of your PA to match the sections in the Requirements (A, B, C... etc.). That way, the evaluators can give very specific feedback to the sections they are looking for. The paper should read (for the most part) as a high-level technical solution recommendations document.

There are 2 sections that ask you to describe internal and external API's. These sections require a more technical detail:

Internal APIs

- i. Describe the technology that the API will be built with (Node js, .Net Core, etc.)
- ii. Where the code will run (AWS Lambda, behind an API Gateway, Azure Functions... etc)
- iii. How the code is invoked (RESTFUL endpoint with parameters... which parameters, etc)
- iv. What happens on invocation (database lookup, calculation, etc)
- v. What is returned (json formatted payload)
- vi. What is done with returned payload

External APIs

- vii. Which third party vendor hosts the API ii. How is the API invoked, what is sent
- viii. What is returned
- ix. What is done with what is returned

A. Authentication Process - Amazon AWS Cognito with User Pools

B. Remote Access - MFA using a dynamic token/physical key (like yubikey)

C. Application Security - Mobile OS for mobile encryption, TLS, public key private key RSA

D. Network Security - VPN TLS

E. Internal API's - Amazon API gateway for all 3

F. External API's - Google Single sign-on SAML, Google Geolocation API, FICO's REST API

G. Deployment plan - I actually had 3 paragraphs just bullshitting about a timeline, what resources, and estimated costs (just pulled it out of my ass)

H. maintenance strategy - patch management monitored and overseen by so and so

I. Disaster Recovery- more mumbo jumbo about disaster potentials and business continuity

J. Regulatory Compliance - basically said that we would follow and be in compliance with SOX and other things mentioned in the supporting bank doc. This was a total word salad 3 sentences long lol

K. Sources - use LastName, FirstName. "Title", Date, URL