Sample Review Response Analysis

Assessment Summary

This review analyzes vendor responses to selected security questionnaire items regarding Multi-Factor Authentication (MFA) policy exceptions. The purpose is to identify gaps, inconsistencies, or areas of concern in the vendor's security posture.

Questionnaire Responses Reviewed

Question 1: What exceptions have been made to your MFA policy?

- **Vendor Answer:** *None*

Question 2: How do you handle MFA on service accounts?

- **Vendor Answer:** *N/A*

Reviewer Assessment

Question	Vendor Answer	Assessment	Comments
Exceptions to MFA policy	None	🔴 **Red Flag**	Service accounts likely cannot support MFA, but no exceptions documented
MFA on service accounts	N/A	🔴 **Red Flag**	Response indicates lack of awareness or governance over service accounts

Analysis

The vendor reported that there are no exceptions to their MFA policy. However, in response to the follow-up question on service accounts, the vendor responded *N/A*.

This response is inconsistent with industry best practices and raises concerns for the following reasons:

- Service accounts typically do not support MFA due to their non-interactive nature. Therefore, organizations with mature security programs usually acknowledge service accounts as an exception to MFA policies.
- Responding “N/A” suggests either that service accounts are unmanaged, that the vendor is unaware of the limitations of MFA on such accounts, or that exceptions have not been properly documented.

This discrepancy indicates a **red flag** and warrants further discussion with the vendor to clarify their practices and ensure appropriate compensating controls are in place.

Recommended Response (🟢 Green Flag Example)

A strong and mature response to these questions would be:

> *We have MFA globally enforced except on service accounts, where MFA is not supported. For service accounts, we enforce strong passwords, restrict permissions to minimum necessary, and monitor usage.*

This answer acknowledges real-world constraints, documents the exception, and describes compensating controls—demonstrating a mature and well-managed security program.
