Security Review Questionnaire for Cloud Service Provider

1. **Does the provider have a documented Information Security Policy?**
   - Yes/No
   - Comments:
2. **Is Multi-Factor Authentication (MFA) required for all access to the platform?**
   - Yes/No
   - Comments:
3. **Are customer data and credentials encrypted at rest and in transit?**
   - Yes/No
   - Comments:
4. **Does the provider conduct regular vulnerability assessments and penetration testing?**
   - Yes/No
   - Comments:
5. **Are security patches and updates applied promptly to all systems?**
   - Yes/No
   - Comments:
6. **Is there a dedicated Security Operations Center (SOC) monitoring the environment 24/7?**
   - Yes/No
   - Comments:
7. **Does the provider have a formal incident response plan in place, and is it regularly tested?**
   - Yes/No
   - Comments:
8. **Are user access rights reviewed and updated regularly?**
   - Yes/No
   - Comments:
9. **Is data backup and recovery testing performed regularly?**
   - Yes/No
   - Comments:
10. **Does the provider comply with industry standards (e.g., ISO 27001, SOC 2, PCI DSS)?**
    - Yes/No
    - Comments:
11. **Are logs retained and monitored for security incidents and anomalies?**
    - Yes/No
    - Comments:
12. **Are personnel subjected to background checks and security training?**
    - Yes/No
    - Comments:

13. **Does the provider have measures in place to detect and prevent malware and ransomware?**
    - Yes/No
    - Comments:
14. **Is there a secure process for onboarding and offboarding users?**
    - Yes/No
    - Comments:
15. **Are network connections protected by firewalls and intrusion detection systems?**
    - Yes/No
    - Comments:
16. **Are there controls in place to prevent data exfiltration?**
    - Yes/No
    - Comments:
17. **Does the provider offer role-based access control (RBAC) to restrict user permissions?**
    - Yes/No
    - Comments:
18. **Are secure software development practices, like Secure SDLC, implemented?**
    - Yes/No
    - Comments:
19. **Does the provider use zero-trust architecture principles for access control?**
    - Yes/No
    - Comments:
20. **Is the provider's infrastructure monitored for configuration drift and compliance violations?**
    - Yes/No
    - Comments: