1. **Data Breach**
   Double-check encryption settings regularly – CSP doesn’t encrypt data stores automatically.

2. **Misconfiguration & Inadequate Change Control**
   Remove default credentials for each service and API you use.

3. **Lack of cloud security architecture & strategy**
   Conduct threat models to ensure efforts are focused on high risk areas.

4. **Insufficient Identity, Access, Key Management**
   Enable role-based access control (RBAC) and/or a second factor for login.

5. **Account Hijacking**
   Create alerts for all new account creations – hackers look for easiest entry point then move laterally.

6. **Insider Threat**
   DLP (data loss prevention) can help flag exfiltration attempts.

7. **Insecure Interfaces & APIs**
   Force input validation for APIs you build and use CSP traffic throttling tools to prevent bot attacks.

8. **Weak Control Plane**
   Reduce number of users who have access and implement RBAC and/or MFA.

9. **Metastructure & Applistructure Failures**
   Monitor security bulletins, patch software and conduct assessments on your own/3rd party apps.

10. **Limited Cloud Usage Visibility**
    Use EASM (external attack surface monitoring) to regularly scan for shadow IT/unsanctioned assets.

11. **Abuse and Nefarious Use of Cloud Services**
    Use CSP monitoring services to identify abnormal resource/employee usage.