Cloud Security Risk Checklist

Critical misconfigurations to fix first in AWS, Azure, or GCP — prioritized by business risk.

📌 Top 5 Cloud Misconfigurations

1. Public S3 buckets
2. Open security groups
3. Unencrypted databases
4. Default admin credentials
5. Lack of MFA

📌 Access Control Best Practices

- Enforce least privilege
- Use IAM roles instead of static keys
- Rotate credentials regularly

📌 Encryption & Monitoring Essentials

- Enable encryption at rest & in transit
- Set up CloudTrail or Azure Monitor
- Automate alerts for critical events

📌 Shared Responsibility Model – Explained

You secure your applications and data; the cloud provider secures the infrastructure.

📌 Checklist for Secure Cloud Environments

✅ MFA enabled
✅ Backups configured
✅ Logging active
✅ No exposed ports

📌 Pro Tips from CISSP Experts

- Review logs weekly
- Scan infrastructure monthly

- Document all security decisions