Cloud IT Security Audit Checklist for Hybrid Infrastructures

A comprehensive **Cloud IT security audit checklist** ensures hybrid infrastructures maintain robust protection against evolving cyber threats. It covers key areas such as access controls, data encryption, and compliance with industry standards. Regular audits help identify vulnerabilities and strengthen overall cloud security posture.

Audit Checklist

- **Access Control**
  - Review role-based access policies (least privilege principle)
  - Enforce multi-factor authentication (MFA)
  - Regularly review and revoke unused accounts
- **Data Security**
  - Verify data-at-rest and data-in-transit are encrypted
  - Check encryption key management policies
  - Ensure backup data is securely stored and encrypted
- **Network Security**
  - Segment networks between cloud and on-premises infrastructure
  - Configure firewalls and security groups properly
  - Monitor for unauthorized connections or access attempts
- **Compliance & Governance**
  - Ensure compliance with relevant standards (e.g., GDPR, HIPAA, ISO 27001)
  - Maintain audit trails and logs for all critical systems
  - Review and update security policies regularly
- **Vulnerability Management**
  - Conduct regular vulnerability scans on cloud and on-premises assets
  - Apply patches and updates in a timely manner
  - Monitor threat intelligence feeds for emerging risks
- **Incident Response**
  - Test incident response plans for cloud and hybrid incidents
  - Ensure contact information for key personnel is up-to-date
  - Document and learn from past incidents
- **Physical Security (for on-premises components)**
  - Restrict physical access to servers and network equipment
  - Monitor with surveillance and access logs
  - Ensure disaster recovery procedures are in place

Tips for Effective Auditing

- Schedule audits periodically (at least annually)
- Engage third-party auditors for unbiased assessments
- Promote cross-team collaboration between IT, Security, and Compliance departments
- Continuously monitor for changes in the threat landscape and update the checklist as needed