Cloud Compliance Audit Checklist

General Information

Organization Name	
Audit Date	
Auditor	
Cloud Service Provider(s)	

1. Access Control

Requirement	Compliant (Yes/No)	Comments
Are user access levels reviewed regularly?		
Is multi-factor authentication enabled?		
Are privileges removed promptly after user departure?		

2. Data Security & Privacy

Requirement	Compliant (Yes/No)	Comments
Is data encrypted at rest and in transit?		
Are backups performed and tested regularly?		
Is there a data retention and deletion policy?		

3. Compliance & Governance

Requirement	Compliant (Yes/No)	Comments
Are relevant compliance frameworks identified?		
Are audits and assessments performed regularly?		
Is there documentation of compliance processes?		

4. Incident Response

Requirement	Compliant (Yes/No)	Comments
Is an incident response plan in place?		
Are incidents recorded and reviewed?		
Is staff trained in cloud incident response?		

5. Vendor Management

Requirement	Compliant (Yes/No)	Comments
Are vendor contracts reviewed for compliance?		
Is there a process for evaluating vendor risk?		
Are service-level agreements (SLAs) monitored?		

5. Vendor Management

Requirement	Compliant (Yes/No)	Comments
Are vendor contracts reviewed for compliance?		
Is there a process for evaluating vendor risk?		
Are service-level agreements (SLAs) monitored?		