

IT Systems Internal Control Evaluation Checklist

Organization:

Date:

Evaluator:

Checklist

Control Area	Control Point	Yes / No / N/A	Comments
Access Controls	Are user access rights reviewed regularly and approval documented?		
	Is there a process for revoking access promptly when users leave or change roles?		
Data Backup & Recovery	Are backups performed according to a standard schedule?		
	Are backup restores tested periodically to ensure reliability?		
Change Management	Are changes to IT systems documented and approved prior to implementation?		
	Is there a rollback plan for all critical changes?		
System Security	Are antivirus and security patches updated regularly?		
	Is there monitoring for unauthorized system or network access?		
Physical & Environmental Controls	Are server rooms access-controlled and monitored?		
	Are there safeguards against fire, flood, and other risks?		
Incident Management	Is there a documented process for incident reporting and investigation?		

Important Notes:

- This checklist should be customized for the specific IT environment.
- Regular updates ensure relevance with changing systems and regulations.
- Proper documentation and evidence collection is critical during evaluation.
- This document supports risk management and compliance activities.
- Involvement from relevant IT and business stakeholders improves accuracy.

