Internal Audit Checklist for IT Systems and Controls

An **internal audit checklist** for IT systems and controls ensures comprehensive evaluation of security measures, compliance, and operational efficiency. It helps identify vulnerabilities and gaps in information technology frameworks, promoting risk mitigation. Regular use of this checklist supports continuous improvement and regulatory adherence.

Sample Internal Audit Checklist

#	Audit Item	Criteria/Objective	Status	Comments/Findings
1	Access Controls	Verify user access rights and role-based permissions are enforced		
2	Data Backup and Recovery	Assess backup frequency, storage, and recovery testing		
3	Patch Management	Check if systems are updated with latest security patches		
4	Network Security	Review firewall, intrusion detection, and network segmentation		
5	Incident Response	Confirm existence and testing of incident response plan		
6	User Training	Evaluate frequency and coverage of IT security training		
7	Compliance	Review adherence to relevant laws, regulations, and standards (e.g., GDPR, ISO 27001)		
8	Change Management	Assess controls for system changes and documentation		
9	Physical Security	Review physical access controls to IT infrastructure		
10	Third-party Vendor Management	Evaluate controls and risk management for external vendors		

Instructions

- Complete each audit item, marking status as 'Compliant', 'Non-Compliant', or 'Not Applicable'.
- Provide detailed comments or findings for each checked item.
- Review the checklist regularly to ensure ongoing compliance and security enhancements.