IT SECURITY AUDIT CHECKLIST

An IT security audit enables companies to review their current security measures, identify weaknesses and evaluate the effectiveness of their IT security strategy. This checklist is divided into eight areas:
Preparation, Technical Security Measures, Organizational Measures, Legal Requirements, Risk Management, Review of Requirements, Performance of Reviews and Analysis of Results.

1. preparation of the IT security audit

Task	Description	Status
Define audit objectives	Which areas should be checked (e.g. network, software, data, employees)?	
	What goal is to be achieved (e.g. improvement of the IT security strategy)?	
Clarify responsibilities	Appointment of an internal or external auditor	
	Ensure that the management is involved	
View documentation	Check security guidelines, protocols, manuals and inventory of the IT infrastructure	

2. check technical safety measures

Task	Description	Status
Network security	Check firewall rules	
	Determine the security status of routers, switches and transceivers	
	Recognize and fix open ports	
Endpoint security	Use antivirus software and password manager	
	Activate two-factor authentication	
Data backup	Test recovery plan	
	Check function and up-to-dateness of backups	
Access rights	Analysis of authorizations	
	Checking and limiting access	
Patch management	Automate updates and run them regularly	

3. check organizational measures

Task	Description	Status
Training and awareness	Regularly train employees on IT security and refresh their knowledge	
Internal communication	Documentation of communication channels	
	Clear policy for internal reporting of incidents	
Security guidelines and processes	Are guidelines for the use of IT resources clearly defined?	
	Is there a process manual for dealing with security incidents?	
Physical security	Check access controls for sensitive areas	
	Use of monitoring systems	

4. check legal requirements

Task	Description	Status
Data protection laws	Check GDPR compliance	
	Are all data processing procedures documented?	
Industry-specific requirements	Ensure compliance with standards (ISO 27001)	
Reporting obligations for security incidents	Is there a concept for notifying the responsible authorities (e.g. BSI)?	
	Are responsibilities clearly defined?	

5. evaluate risk management

Task	Description	Status
Risk assessment	Identification of potential risks (e.g. ransomware, phishing)	
	Assessment of the probability of occurrence	
Response plans for security incidents	Are there instructions for action in the event of an emergency (e.g. hacker attack)?	
	Are internal and external contacts clearly named?	
Regular safety audits	Definition of an audit cycle (e.g. annually)	
	Ensuring measures and improving audit results	

6. examination of legal and regulatory requirements

Task	Description	Status
Data protection (DSGVO) and industry standards	Is personal data processed and stored correctly?	
	Is there a procedure for reporting data breaches?	
	Are reporting obligations in the event of cyber attacks known and documented?	

7. carrying out security checks

Task	Description	Status
Penetration tests and vulnerability analyses	Hiring white-hat hackers to find vulnerabilities	
	Are there any reports of security vulnerabilities and how to fix them?	
Simulated attacks and emergency scenarios	How quickly do you react to simulated attacks?	
	Are there clear processes for restoring systems systems after an incident?	

8. results analysis and documentation

Task	Description	Status
Create audit report	Summary of the identified weaknesses	
	Are there prioritized recommendations for action?	
Develop action plan and follow-up	Are steps being taken to eliminate vulnerabilities?	
	Is there a plan for future audits?	

This checklist helps to holistically assess the state of IT security, identify strengths and weaknesses and take targeted measures. A regular audit helps to raise security standards and strengthen resilience against cyber attacks.

Tip: Use tools and frameworks such as the BSI baseline protection compendium or ISO 27001 for structured audits. This will ensure that your IT security complies with current standards and that potential risks are minimized.