



IT

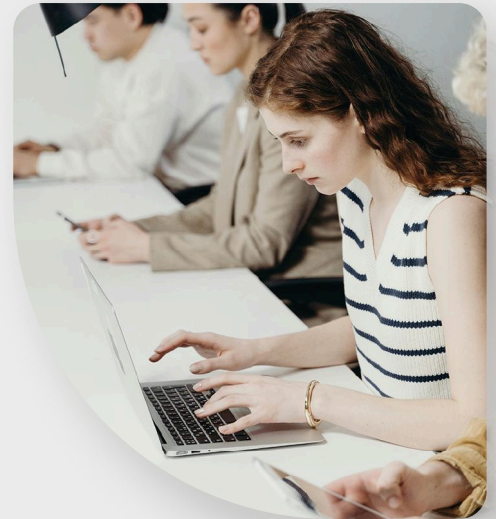
Audit Checklists

Here you will find **two checklists** to assist your **IT audit process**.

The first is a general audit checklist with the main steps to follow in every audit process. The second will guide you through your efforts with questions covering with sample questions related to the typical IT audit areas.

Good luck!

A general IT audit process checklist



@ People involved

📅 Due Date

1 Planning

☐

Define the audit scope and objectives.

☐

Conduct a preliminary risk assessment.

☐

Develop the audit plan.

☐

Select the audit team.

☐

Communicate the audit details with stakeholders.

☐

Review previous audit findings.

☐

Gather and review preliminary data.

☐

Schedule audit activities.

☐

Prepare any necessary audit tools and resources.



* More details on some of these planning steps are included in the following two sections.

2 Preliminary review

☐

Conduct background research and information gathering.

☐

Hold initial meetings and communication.

☐

Review IT policies, processes and procedures.

☐

Understand the IT infrastructure and environment.

☐

Identify key IT processes and their maturity.

☐

Review previous audits and assessments.

☐

Consider the need for regulatory and compliance review audit elements.

☐

Begin identifying potential risks and areas of concern in the IT environment.

☐

Start planning the detailed audit work.

☐

Document findings, observations, and insights gained during the preliminary review.



3 Risk assessment

☐

Discover potential threats and identify vulnerabilities.

☐

Assess vulnerabilities.

☐

Evaluate and prioritize risks.

☐

Review existing controls and identify control gaps.

☐

Apply risk treatments – mitigation strategies and recommended controls.

☐

Apply risk treatments – mitigation strategies and recommended controls.



- | | | | |
|--------------------------|--|---|---|
| <input type="checkbox"/> | Document the risk assessment findings. | @ | 1 |
| <input type="checkbox"/> | Communicate the risk assessment results. | @ | 1 |
| <input type="checkbox"/> | Review and update risks over time. | @ | 1 |

4 Fieldwork and testing

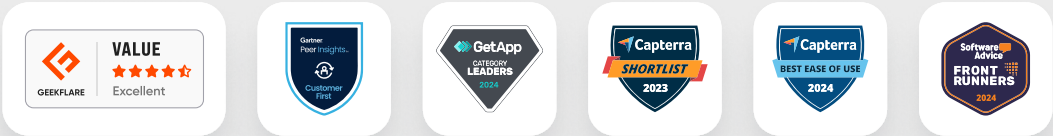
- | | | | |
|--------------------------|---|---|---|
| <input type="checkbox"/> | Conduct tests and evaluations using audit techniques such as sampling, observation, and data analysis. | @ | 1 |
| <input type="checkbox"/> | Gather and document evidence. | @ | 1 |
| <input type="checkbox"/> | Evaluate and prioritize risks. | @ | 1 |
| <input type="checkbox"/> | Reviewing documentation such as policies, procedures, and other documentation relevant to the IT audit scope. | @ | 1 |
| <input type="checkbox"/> | Conduct technical assessments such as vulnerability scanning, penetration testing, and configuration reviews. | @ | 1 |
| <input type="checkbox"/> | Assess compliance with relevant laws, regulations, and industry standards. | @ | 1 |
| <input type="checkbox"/> | Evaluate the effectiveness of controls | @ | 1 |
| <input type="checkbox"/> | Identify risks and issues. | @ | 1 |


5 Reporting

- | | | | |
|--------------------------|--|---|---|
| <input type="checkbox"/> | Compile the audit findings and evidence. | @ | 1 |
| <input type="checkbox"/> | Draft the report and include recommendations and action plans. | @ | 1 |
| <input type="checkbox"/> | Review and quality check the draft report. | @ | 1 |
| <input type="checkbox"/> | Finalize the report, incorporating stakeholder feedback. | @ | 1 |





<input type="checkbox"/>	Distribute and communicate the report.	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Follow-up and monitor the implementation of audit recommendations.	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Develop a contingency plan based on potential issues.	<input type="text"/>	<input type="text"/>

** Please remember that this IT audit process checklist needs to be tailored to your audit needs and circumstances*






InvGate
Asset Management

Take a test run of the best ITAM software out there

Discover first-hand what InvGate looks like in action.
Scan the code and take a self-guided tour of InvGate Asset Management



Product tour

InvGate is a great fit for organizations of all sizes and industries



A general IT audit question checklist



@ People involved

📅 Due Date

1 IT governance and policy

@

📅

☐

Are IT policies and procedures well-documented and communicated?

@

📅

☐

Is there an IT governance framework in place that aligns with organizational objectives?

@

📅

2 Network security

@

📅

☐

Are corporate firewalls, intrusion detection/prevention systems, and antivirus software implemented and up-to-date?

@

📅

☐

Are network security configurations regularly reviewed and tested?

@

📅

3 Access controls

@

📅

☐

Are strong password policies enforced?

@

📅

☐

Is there a process for managing user accounts and permissions, including timely deactivation for terminated employees?

@

📅

4 Data protection

☐

Is sensitive data encrypted during transmission and storage?

☐

Are data backup and restoration procedures in place and tested regularly?



5 Physical security

☐

Are there controls to prevent unauthorized physical access to IT facilities?

☐

Is there environmental protection (e.g. against fire and flooding) for critical IT assets?



6 Disaster recovery and business continuity

☐

Is there a documented and tested disaster recovery plan?

☐

Is there a business continuity plan in place to ensure IT services continuity during emergencies?



7 Application security

☐

Are applications regularly tested for security vulnerabilities?

☐

Is there a process for timely application patching and updates?



8 Vendor Management

☐

Are vendor risk assessments conducted?

☐

Are there contracts and agreements that include security and confidentiality clauses with all third-party service providers?



9 Employee IT security training and awareness



☐ Is there an ongoing cybersecurity awareness training program for employees?



☐ Are employees aware of their roles and responsibilities regarding information security?



10 Incident response



☐ Is a documented incident response plan in place, and is it tested regularly?



☐ Are incidents and breaches documented and analyzed for lessons learned?



11 Compliance



☐ Is the organization compliant with applicable regulatory and legal requirements?



☐ Are regular compliance assessments conducted to ensure continuous adherence to regulations?



12 System Patch Management



☐ Is there a process for identifying and applying necessary system patches and updates?



☐ Are systems regularly scanned for vulnerabilities?



13 Audit logs and monitoring



☐ Are audit logs collected, reviewed, and securely stored?



☐ Is there a process for monitoring and responding to suspicious activities?



14 Asset Management

☐

Is there an up-to-date inventory of IT assets?

☐

Are Asset Management procedures in place for the lifecycle of assets, including disposal?



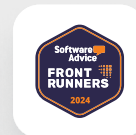
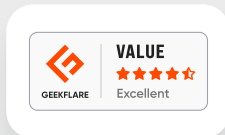
15 Cloud security

☐

Are there security controls in place for cloud services and data stored in the cloud?

☐

Is there a documented policy for the use of cloud services?



InvGate
Asset Management

Take a test run of the best ITAM software out there



Discover first-hand what InvGate looks like in action.
Scan the code and take a self-guided tour of InvGate Asset Management



Product tour

InvGate is a great fit for organizations of all sizes and industries

