Checklists

Auditoria de TI

Aqui você encontrará **dois checklists para ajudar no seu processo de auditoria de TI.**

O primeiro é um checklist geral com as principais etapas a serem seguidas em qualquer processo de auditoria. O segundo irá guiá-lo com perguntas de exemplo relacionadas às áreas típicas de uma auditoria de TI.

Boa sorte!

InvGate
Asset Management

Baixar checklist geral para o processo de auditoria de TI

Ao realizar uma auditoria de TI, este checklist ajudará a garantir que as etapas-chave sejam cobertas.

Pessoas envolvidas | Data de entrega

1 Planejamento

- [ ] Definir o escopo e os objetivos da auditoria.
- [ ] Realizar uma avaliação preliminar de riscos.
- [ ] Desenvolver o plano de auditoria.
- [ ] Selecionar a equipe de auditoria.
- [ ] Comunicar os detalhes da auditoria com as partes interessadas.
- [ ] Revisar as constatações de auditorias anteriores.
- [ ] Coletar e revisar dados preliminares.
- [ ] Programar atividades de auditoria.
- [ ] Preparar todas as ferramentas e recursos necessários para a auditoria.

** Mais detalhes sobre algumas dessas etapas de planejamento estão incluídos nas próximas duas seções.*

2 Revisão preliminar

- [ ] Realizar pesquisa preliminar e coleta de informações.
- [ ] Realizar reuniões e comunicações iniciais.
- [ ] Revisar políticas, processos e procedimentos de TI.
- [ ] Entender a infraestrutura e o ambiente de TI.
- [ ] Identificar processos-chave de TI e sua maturidade.
- [ ] Revisar auditorias e avaliações anteriores.
- [ ] Considerar a necessidade de elementos de auditoria de revisão regulatória e de conformidade.
- [ ] Começar a identificar riscos potenciais e áreas de preocupação no ambiente de TI.
- [ ] Começar a planejar o trabalho detalhado de auditoria.
- [ ] Documentar constatações, observações e ideias obtidas durante a revisão preliminar.

3 Avaliação de riscos

- [ ] Descobrir ameaças potenciais e identificar vulnerabilidades.
- [ ] Avaliar vulnerabilidades.
- [ ] Avaliar e priorizar riscos.
- [ ] Revisar controles existentes e identificar lacunas nos controles.
- [ ] Aplicar tratamentos de risco: estratégias de mitigação e controles recomendados.

- [ ] Documentar as constatações da avaliação de riscos.
- [ ] Comunicar os resultados da avaliação de riscos.
- [ ] Revisar e atualizar riscos ao longo do tempo.

4 Trabalho de campo e testes

- [ ] Realizar testes e avaliações utilizando técnicas de auditoria como amostragem, observação e análise de dados.
- [ ] Coletar e documentar evidências.
- [ ] Realizar entrevistas e questionários.
- [ ] Revisar documentação como políticas, procedimentos e outra documentação relevante para o escopo da auditoria de TI.
- [ ] Realizar avaliações técnicas como varredura de vulnerabilidades, testes de penetração e revisões de configuração.
- [ ] Avaliar a conformidade com leis, regulamentos e padrões da indústria relevantes.
- [ ] Avaliar a eficácia dos controles.
- [ ] Identificar riscos e problemas.

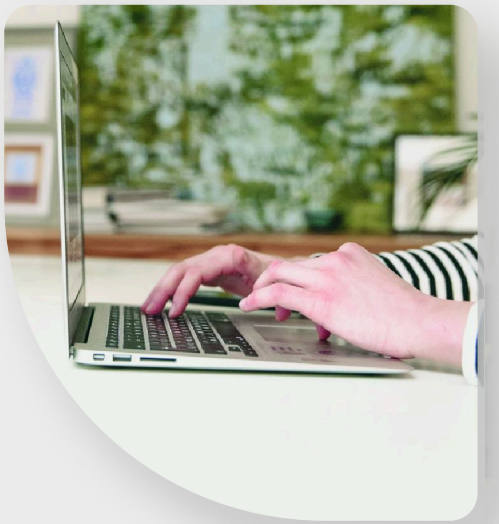
5 Relatório

- [ ] Compilar as constatações e evidências da auditoria.
- [ ] Redigir o relatório e incluir recomendações e planos de ação.
- [ ] Revisar e verificar a qualidade do relatório preliminar.
- [ ] Fornecer o relatório preliminar às partes interessadas para revisão e feedback.

☐	Finalizar o relatório, incorporando o feedback das partes interessadas.		
☐	Distribuir e comunicar o relatório.		
☐	Acompanhar e monitorar a implementação das recomendações da auditoria.		
☐	Desenvolver um plano de contingência baseado em problemas potenciais.		

** Lembre-se de que é necessário adaptar este checklist de auditoria de TI às suas necessidades e circunstâncias específicas de auditoria.*

Baixar checklist geral de perguntas para uma auditoria de TI



Este checklist geral de auditoria de TI cobre vários aspectos do ambiente de TI de uma organização, com perguntas de amostra relacionadas às áreas típicas de auditoria.

Pessoas envolvidas | Data de entrega

1 Governança e políticas de TI

- [ ] As políticas e procedimentos de TI estão bem documentados e comunicados?
- [ ] Existe uma estrutura de governança de TI que se alinha com os objetivos organizacionais?

2 Segurança de rede

- [ ] Os firewalls corporativos, sistemas de detecção/prevenção de intrusões e software antivírus são implementados e atualizados?
- [ ] As configurações de segurança da rede são revisadas e testadas regularmente?

3 Controles de acesso

- [ ] Políticas de senhas seguras são aplicadas?
- [ ] Existe um processo para gerenciar contas de usuário e permissões, incluindo a desativação oportuna para funcionários demitidos?

4 Proteção de dados

- [ ] Os dados sensíveis são criptografados durante a transmissão e o armazenamento?
- [ ] Existem procedimentos de backup e restauração de dados, e são testados regularmente?

5 Segurança física

- [ ] Existem controles para prevenir o acesso físico não autorizado às instalações de TI?
- [ ] Existe proteção ambiental (por exemplo, contra incêndios e inundações) para ativos críticos de TI?

6 Recuperação de desastres e continuidade de negócios

- [ ] Existe um plano de recuperação de desastres documentado e testado?
- [ ] Existe um plano de continuidade de negócios para garantir a continuidade dos serviços de TI durante emergências?

7 Segurança de aplicações

- [ ] As aplicações são testadas regularmente em busca de vulnerabilidades de segurança?
- [ ] Existe um processo para a aplicação oportuna de patches e atualizações de aplicações?

8 Gestão de fornecedores

- [ ] São realizadas avaliações de riscos de fornecedores?

- [ ] Existem contratos e acordos que incluem cláusulas de segurança e confidencialidade com todos os fornecedores de serviços externos?

9 Treinamento e conscientização sobre segurança de TI para funcionários

- [ ] Existe um programa de treinamento contínuo sobre conscientização em cibersegurança para funcionários?
- [ ] Os funcionários estão cientes de seus papéis e responsabilidades quanto à segurança da informação?

10 Resposta a incidentes

- [ ] Existe um plano de resposta a incidentes documentado e é testado regularmente?
- [ ] Os incidentes e violações são documentados e analisados para aprendizado de lições?

11 Conformidade

- [ ] A organização cumpre os requisitos regulatórios e legais aplicáveis?
- [ ] São realizadas avaliações periódicas de conformidade para garantir a conformidade contínua com as regulamentações?

12 Gerenciamento de patches de sistema

- [ ] Existe um processo para identificar e aplicar patches e atualizações de sistema necessários?
- [ ] Os sistemas são regularmente verificados em busca de vulnerabilidades?

13 Registros de auditoria e monitoramento

- [ ] Os registros de auditoria são coletados, revisados e armazenados com segurança?
- [ ] Existe um processo para monitorar e responder a atividades suspeitas?

14 Gestão de ativos

- [ ] Existe um inventário atualizado de ativos de TI?
- [ ] Os procedimentos de Gestão de Ativos são aplicados ao ciclo de vida dos ativos, incluindo à disposição?

15 Segurança na nuvem

- [ ] Existem controles de segurança para os serviços em nuvem e os dados armazenados na nuvem?
- [ ] Existe uma política documentada para o uso de serviços em nuvem?