Exercício de auditoria ISO27k

Contribuição ao ISO27k Toolkit
por Jerry Lai e Gary Hinson

Setembro 2021

Introdução

O proposito deste exercício é de praticar a escrita de um relatório de auditoria da ISO 27001. Desta maneira, você poderá melhorar suas habilidades sobre o assunto.

Instruções

Para este exercício, a tabela abaixo possui 19 apontamentos de auditoria – em uma auditoria real, essa quantidade pode variar de acordo com o cenário da empresa auditada. Imagine que você executou uma auditoria interna, passou por um processo de certificação da ISO/IEC 27001, por uma Análise Crítica da Alta Direção ou algum processo semelhante, onde esses apontamentos foram gerados. **Complete a tabela como se você estivesse reportando o resultado para a Alta Direção,** considerando as seguintes colunas:

- **Requisito**: qual o requisito(s) da ISO/IEC 27001:2013 é ou são mais relevante(s)
- **Categoria**:
  - **NC** = Não conformidade maior – falha em não atender de forma completa exigências de um requisito da ISO/IEC 27001. **DEVEM** ser tratadas de forma prioritária para que a organização possa se certificar;
  - **nc** = Não conformidade menor – uma falha de menor relevância da organização frente a algum requisito da ISO/IEC 27001. DEVE ser tratada em um prazo maior do que a NC, mas, não é impeditivo para obter a certificação;
  - **obs** = observações da auditoria – não é uma não conformidade, trata-se mais de um comentário ou sugestão de oportunidade de melhoria de como a organização escolheu e implementou o Anexo A ou outros controles;
  - **irr** = irrelevante e provavelmente fora do escopo da auditoria.
- **Impacto**: possível impacto potencial causado a organização, caso nada seja feito para resolver o problema.
- **Recomendações**: o que você recomendaria para solucionar os pontos identificados (Nota: o que será feito, não é decidido pelo auditor(a), e sim pelo cliente, mas, se o auditor(a) na Auditoria de Certificação não estiver satisfeito(a) com a resposta, ele/ela pode não recomendar a certificação a autoridade certificadora, enquanto os pontos não forem solucionados.

Como o contexto é importante, você pode achar útil, prever o que poderia encontrar em auditoria em um determinado setor, considerando o tamanho, complexidade e maturidade da empresa – não necessariamente a sua empresa atual ou de seus clientes! Além disso, em algumas situações, políticas de

auditoria e práticas da produção do relatório pode variar entre organizações. Ex: alguns auditores não chegam a fazer recomendações, deixando a Alta Direção responsável por decidir o que (se houver) fazer em resposta aos resultados da auditoria. Este exercício é genérico.

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impacto	Recomendações
1. Os critérios usados para avaliar os riscos não são atualizados desde o ano passado		NC/nc/obs/irr		
2. O acesso a uma pasta que deveria ser restrita está sendo compartilhada com todos na organização		NC/nc/obs/irr		
3. Auditoria de campo indica que a conscientização no departamento de segurança é baixa (abaixo de 50%, usando como base a própria métrica da organização)		NC/nc/obs/irr		
4. Alguns softwares que estão em uso não foram adequadamente testados, devido à ausência de requisitos pré-		NC/nc/obs/irr		

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impacto	Recomendações
estabelecidos de segurança				
5. Políticas do Sistema de Gestão não possuem um controle de versão e registro de distribuição de acesso		NC/nc/obs/irr		
6. O departamento de Marketing está trabalhando no lançamento de um produto em conjunto com um fornecedor (agência de propaganda) a qual não tem um NDA assinado		NC/nc/obs/irr		
7. O fornecimento de recursos ao Sistema de Gestão de Segurança da Informação (SGSI) é muito restrito		NC/nc/obs/irr		
8. Contas inativas de rede não são desabilitadas conforme políticas e procedimentos interno		NC/nc/obs/irr		

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impacto	Recomendações
9. O uso de senhas fracas é comum		NC/nc/obs/irr		
10. O controle de versão do documento “Registro de Ativos de Informação” mostra que a última atualização do documento foi há 5 anos atrás		NC/nc/obs/irr		
11. Documentos confidenciais são armazenados em notebooks pessoais ao invés de ser guardados no meio de armazenamento corporativo autorizado		NC/nc/obs/irr		
12. Nenhuma evidência da execução da avaliação de riscos à segurança da informação foi apresentada		NC/nc/obs/irr		

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impacto	Recomendações
13. Contas inativas de rede não são desabilitadas e permanecem ativas de forma indefinida		NC/nc/obs/irr		
14. Nenhuma solução de antivírus está sendo usada		NC/nc/obs/irr		
15. Embora a organização não processe dados de cartões, não realiza auditoria de conformidade com o PCI para indicar um possíveis falhas no tratamento de dados pessoais		NC/nc/obs/irr		
16. Quando questionados, alguns colaboradores mostram desconhecimento da política de segurança da organização		NC/nc/obs/irr		

Resumo dos apontamentos da Auditoria	Cláusula	Categoria	Impacto	Recomendações
17. A organização não possui contato com grupos especiais (fóruns, boletins, newsletter, eventos e etc) para se atualizar sobre assuntos relacionados à segurança da informação		NC/nc/obs/irr		
18. Ao menos uma NC não foi tratada desde a última auditoria		NC/nc/obs/irr		
19. Alguns incidentes relacionados a privacidade identificados não foram reportados conforme processo estabelecido internamente		NC/nc/obs/irr		
*** Fim do Exercício ***				

O "Material de Anotações" do kit da ISO27k possui sugestões e modelos de respostas

Tente sozinho completar o exercício! Deixe para abri-lo somente no final, como comparativo ao que você fez.

Questões extras

- Revise e comente sobre a forma de escrita, gramática e compreensão dos apontamentos descritos na coluna “Resumo dos apontamentos da Auditoria”.
- Qual tipo de evidência você gostaria de receber para cada um dos apontamentos identificados?
- Revise todos os apontamentos usando, por exemplo, a Análise SWOT, e escreva onde cada um deles se encaixa no método.
- Se você tivesse que retirar um dos apontamentos, qual deles você manteria/removeria e por qual motivo? Explique seu raciocínio.
- Se você for questionado sobre informações adicionais ou demais recomendações, qual outra norma da família 27000 ou outro padrão/framework de segurança você acha que seria pertinente a organização adotar?
- Envie feedbacks sobre o exercício ou sobre o material de anotações para os autores, Jerry Lai e Gary Hinson. Sugestões de melhoria são sempre bem-vindas. Por favor, evite apenas comentar ou discutir sobre nas redes sociais, de maneira que, as pessoas que não ainda não fizeram o exercício, possa fazê-lo sem ter acesso as respostas.