ISO27k audit exercise

Contributed to the ISO27k Toolkit
by Jerry Lai and Gary Hinson

September 2021

Introduction

The purpose of this exercise is to practice reporting on ISO27k audits and so refine your skills, learning and improving.

Instructions

The table below contains 19 audit findings for this exercise – more than would normally be the case in a genuine audit. Imagine that you that you have performed an ISMS internal audit, ISO/IEC 27001 certification audit, ISMS management review, or something similar, generating these issues. **Complete the remainder of the table as if you were reporting these findings to management**, under the following columns:

- **Clause**: which clause/s of ISO/IEC 27001:2013 is/are (most) relevant - if any?
- **Category**:
  - **NC** = Major non-compliance - a complete, blatant or serious failure to do whatever a main body clause of ISO/IEC 27001 requires. This ***MUST*** be resolved as a priority in order for the organization to be certified;
  - **nc** = Minor non-compliance - a relatively minor discrepancy between the organization and a '27001 main body clause. This *SHOULD* be resolved as soon as practicable, but may not prevent certification;
  - **obs** = audit observation - not a noncompliance as such, more a helpful comment or improvement suggestion, such as issues with the way the organization has chosen and implemented Annex A or other controls;
  - **irr** = irrelevant to, and probably out of scope of, a typical ISO27k audit.
- **Impact**: potential, possible or likely outcome for the organization if nothing is done to address and resolve this issue.
- **Recommendations**: what you might suggest ought to be done to resolve this issue (note: ultimately the client decides, not the auditor, but if a certification auditor isn't happy with the response, he/she may refuse to certify until/unless the issue is resolved).

Since the context is important, you may find it helpful to envisage auditing an organization of a specific type, size, complexity and maturity, in a given industry – not necessarily your current employer or clients! Also, auditing policies and reporting practices vary between organizations and situations *e.g.* some audit functions stop short of making recommendations, leaving management entirely responsible for deciding what (if anything) to do in response to the audit findings. This exercise is generic.

Summary audit finding	Clause	Category	Impact	Recommendations
1. The criteria for evaluating information risks have not been updated since last year		NC/nc/obs/irr		
2. A restricted folder is being shared for everyone to access		NC/nc/obs/irr		
3. Audit fieldwork indicates that security awareness for Finance Department is poor (below 50%, using the organization's own awareness metrics)		NC/nc/obs/irr		
4. Some software in use has not been adequately security tested, due to the lack of security requirements specifications to test against and other deficiencies or constraints		NC/nc/obs/irr		

Summary audit finding	Clause	Category	Impact	Recommendations
5. ISMS policies are not version-controlled, with no record of their distribution and access		NC/nc/obs/irr		
6. Marketing Department is working on new product launches in conjunction with a professional services supplier (an advertising agency) that has not signed a Non-Disclosure Agreement		NC/nc/obs/irr		
7. The ISMS is severely and unnecessarily resource-constrained		NC/nc/obs/irr		
8. Leavers' network accounts are not promptly disabled as required in the leavers' procedures and policies		NC/nc/obs/irr		

Summary audit finding	Clause	Category	Impact	Recommendations
9. Weak passwords are commonplace		NC/nc/obs/irr		
10. The document control in the Information Asset Register shows the last update was 5 years ago		NC/nc/obs/irr		
11. Confidential business documents are stored in a manager's personal laptop instead of the company's dedicated secured storage		NC/nc/obs/irr		
12. No *evidence* of information risks being formally evaluated		NC/nc/obs/irr		
13. Leavers' network accounts are not promptly disabled and some remain active indefinitely		NC/nc/obs/irr		

Summary audit finding	Clause	Category	Impact	Recommendations
14. No antivirus package is in use		NC/nc/obs/irr		
15. Although the organisation does not actually process credit cards, it does not conduct regular PCI compliance audits that might indicate issues with its handling of personal data		NC/nc/obs/irr		
16. When questioned, some workers were substantially ignorant of the organization's information security policy		NC/nc/obs/irr		
17. The organization has little if any contact with industry peers and other local businesses on information security matters		NC/nc/obs/irr		

Summary audit finding	Clause	Category	Impact	Recommendations
18. At least one NC from previous audits remains unresolved		NC/nc/obs/irr		
19. Some privacy issues have not been reported promptly through the designated reporting mechanisms		NC/nc/obs/irr		
*** End of exercise ***				

The 'crib sheet' in the ISO27k Toolkit has suggested/model answers

Don't open it, though, until you have completed the exercise. No cheating!

Optional extras

For bonus marks:

- Review and comment on, or revise, the wording of the summary audit findings for grammar/readability, accuracy and relevance.
- What supporting evidence would you expect to have on file for each of the findings?
- Evaluate the findings as a whole (*e.g.* using a SWOT analysis) and write the remainder of the audit report accordingly.
- If you had to drop some of these findings, which would you remove/retain, and why? Explain your rationale.
- If you were asked for additional information or advice on any of these findings and recommendations, what ISO27k or other standards, advisories or methods (if any) would be pertinent?
- Send feedback on the exercise and crib sheet to the authors, Jerry Lai and Gary Hinson. Improvement suggestions are very welcome. Please avoid raising and discussing specifics on social media *etc*. so as not to tip-off other students who have yet to do the exercise and learn the ropes.