ISO27k audit exercise

Crib sheet

These are *model* answers to the ISO27k audit exercise. You may not agree with these suggestions and you may well be right, not least because the organizational context or situation markedly affects things (*e.g.* many of the information risks and hence controls needed by a small law firm are quite different to, say, a large, mature defence contractor).

Remember: the primary objective of this exercise is to practice the process and refine your auditing skills, learning and improving.

There are explanatory notes beneath the table.

Summary audit finding	Clause	Category	Impacts	Recommendations
1. The criteria for evaluating information risks have not been updated since last year	6.1.2 (a)(1)	**NC**	The information risk criteria and hence assessed risks may not reflect the *current* business situation	Check and either reaffirm or revise and apply the criteria before the end of this year
2. A restricted folder is being shared for everyone to access	A.9.2.2	**nc**	Unclear accountability if an unauthorized access incident occurs	Create/refine an access control policy clarifying who is accountable for determining who should have what kind of access to information; implement the policy through procedures documenting the processes for assigning accountabilities to suitable individuals
3. Audit fieldwork indicates that security awareness for Finance Department is poor (below 50%, using the organization's own awareness metrics)	7.3 + A7.2.2	**NC/nc** (auditor decides according to materiality)	With insufficient awareness, workers are more vulnerable (easy targets!) for phishing/social engineering/malware attacks, frauds, coercion *etc*. and are less likely to comply with policies	Ensure periodic security awareness/training is provided for workers, according to their individual and the organization's general needs; use assessments, surveys and other metrics to both gauge and drive up understanding, reducing the vulnerabilities; adjust the awareness content and delivery to suit the audiences e.g. introduce financial incident examples in the awareness & training materials for Finance workers

Summary audit finding	Clause	Category	Impacts	Recommendations
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/constraints	A.14.2.5	**obs**	The implications depend on the nature of the software, its use, and the possible security flaws	Identify and prioritise the testing of critical applications; review the information risks in this area; have the relevant risk or application owners *formally and explicitly* accept the residual information risks associated with non-critical apps
5. ISMS policies are not version-controlled, with no record of their distribution and access	7.5.3	**NC**	People may be using out-of-date policies and missing out on changes including new ones	Implement a process to ensure that new/updated policies and related procedures, guidelines etc. are circulated to the right people at the right time, and any previous versions are formally withdrawn e.g. using a controlled area on the corporate intranet
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	A.13.2.4	**nc**	Sensitive business information is being released to the vendor without the appropriate controls in place; premature or inappropriate disclosure of the information is likely to cause reputational harm and loss of revenue	In accordance with the security policy, external parties must formally commit to a suitable NDA *before* being given access to information classified 'confidential'; further assurance controls may also be appropriate to ensure they comply with the obligations to protect, use and not disclose the information inappropriately; this audit finding relates to an incident that should be handled through the incident management process
7. The ISMS is severely and unnecessarily resource-constrained	5.1 (c)	**NC**	The ISMS cannot achieve its objectives, at least not in a *reasonable* timescale	In conjunction with top management, revisit the objectives and the value proposition for the ISMS, leading to more realistic objectives *and* adequate resourcing to achieve them
8. Leavers' network accounts are not promptly disabled as required in the leavers' procedures and policies	A.9.2.1	**nc**	Leavers may retain and exploit their access to the network	Measure and drive up compliance with the policies and procedures through better training, clear management direction, plaudits for compliance, penalties for non-compliance etc.

Summary audit finding	Clause	Category	Impacts	Recommendations
9. Weak passwords are commonplace	A.9.4.3	**obs**	The organization's access control and accountability objectives are unlikely to be satisfied, leaving the associated information risks inadequately treated	Prepare, release and mandate a password policy plus complexity standards; accompany the policy with procedures and awareness/training activities for IT users *and* system admins; periodically check for policy compliance, dealing with any issues accordingly
10. The document control in the Information Asset Register shows the last update was 5 years ago	6.1.2(b) + A.8.1.1	**NC**	The current IAR is inaccurate and potentially missing important assets that should be identified, risk-assessed and treated	Review information assets and the associated risks periodically (e.g. every 1-3 years depending on volatility) in accordance with the ISMS requirements, updating the relevant registers accordingly
11. Confidential business documents are stored in an manager's personal laptop instead of company's dedicated secured storage	A.8.1.1	**nc**	Typical incidents such as theft, loss, hardware failure or malware infection of the laptop may inappropriately disclose or prevent legitimate access to the information, causing business issues, losses and costs; the risks would be lower if the secure storage was used as intended	Review the information risks and security controls applicable to 'confidential' business documents; strengthen compliance through awareness, training, technical compliance checks, audits, management oversight etc.
12. No *evidence* of information risks being formally evaluated	8.2	**NC**	Distinct possibility that some information risks are inadequately treated	Revise the risk management process to evaluate all identified information risks *and* retain relevant supporting evidence (formalise the process)
13. Leavers' network accounts are not promptly disabled and some remain active indefinitely	A.9.2.1	**Obs**	Leavers may retain and exploit their access to the network	Revisit, evaluate and treat information risks relating to leavers, accountability, access control *etc.* through appropriate policies, procedures and technical controls
14. No antivirus package is in use	A.12.2	**Obs**	Increased risk of malware infections - more and perhaps more severe incidents likely	Revisit, evaluate and treat malware-related risks, retaining documentary evidence of the associated decisions and actions arising

Summary audit finding	Clause	Category	Impacts	Recommendations
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	None or possibly A.12.6.1 and A.18.1.4	**irr**	[This is an example of an audit finding reflecting the auditor's *personal* prejudices or expectations, rather than the ISO/IEC standard's requirements and recommendations, or the organisation's]	[This kind of audit finding *may* be worth discussing and perhaps progressing, but is probably not relevant to the ISMS and its certification hence it is probably out of scope of the ISO27k audit. Management may choose to ignore it, or perhaps bear it in mind and maybe take it forward separately, and/or remind the auditor of the scope and purpose of the present audit.]
16. When questioned, some workers were substantially ignorant of the organization's information security policy	7.3 + A.7.2.1	**NC/nc** depending on materiality (significance)	Employees and organization are exposed to the security risk of losing organization's data and other valuable assets	Through suitable assurance arrangements (*e.g.* surveys, tests, checks), management should ensure all workers are sufficiently aware of the policy and their obligations through awareness and training activities, clauses in employment contracts/service agreements etc.
17. The organization has little if any contact with industry peers and other local businesses on information security matters	4.1 + A.6.1.4	**NC**	The organization is probably out of touch with recent/ongoing incidents and challenges in its industry and area	Understanding the business context - both internally and external to the organization - is an essential part of information risk and security management … so establish social links, attend forums and generally engage with applicable communities of interest
18. At least one NC from previous audits remains unresolved	10.1 + A.18.2.2	**NC**	The organization cannot be (re)certified with major noncompliances	Top management should prioritise and resource the resolution of NCs appropriately, re-affirming the importance of and their support for the ISMS
19. Some privacy issues have not been reported promptly through the designated reporting mechanisms	A.16.1.2	**Obs**	Delayed responses to incidents and near-misses reduces efficiency and effectiveness e.g. by limiting managements choices of how to respond	Whereas it would be unreasonable to insist that *all* incidents are instantly reported, prompt reporting of [potentially] serious incidents can markedly improve the speed and efficiency of the incident responses; this finding suggests an ISMS improvement opportunity

About the wording

Some of the summary findings, impacts and recommendations in the table are vaguely worded and, without more context, might be misunderstood, doubted or challenged by management. Findings would normally be supported by audit evidence and analysis held on file, ideally indexed and referenced from the audit report or (if reasonably succinct) appended to it. Presenting and discussing the draft audit report with management is an excellent opportunity to bring up and address such issues, and ideally gain the organization's commitment to the actions arising, before finalising it.

About category

- **NC** = 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, as it indicates that the ISMS is not designed and functioning as specified by the standard.
- **nc** = a relatively minor discrepancy between the organization and a '27001 main body clause, for example insufficient hard evidence that the proper ISMS processes (as specified in the main body of '27001) have in fact been followed. This *should* be addressed and ideally resolved as soon as practicable, but *may* not prevent certification.
- **obs** = not strictly a noncompliance so much as a helpful comment or improvement suggestion. Concerns about the organization's analysis, decisions and treatment of its information risks are generally observations. The auditor may have an opinion, and '27001 Annex A or other control catalogues may suggest a different approach, but *management* has the right to decide what to do. Provided they followed their ISMS processes, and provided those processes fulfil the '27001 main body requirements, differences of opinion or approach on the security controls *etc*. are *not* sound reasons to withhold certification.
- **irr** = irrelevant to, and probably out of scope of, a typical ISO27k audit. Information security management is such a broad topic that almost anything relating to the protection of information *could* be deemed relevant, but that's not helpful if the central purpose of the audit is to review the ISMS for compliance with '27001. Such issues can be distracting and may be handled informally, perhaps set aside to be picked up later in other audits, reviews *etc*.

About impacts

Remember that the main objective of an ISMS is to help the organization manage the arrangements necessary to protect valuable information against various risks, in ways that benefit the business. Compliance with '27001 is merely a means to that end, not an end in itself. Describing impacts in business terms reinforces that distinction, especially if they are clearly of concern to management.

About recommendations

Ultimately management/the client (not the auditor!) decides how to address the findings … but if a certification auditor isn't happy with the response, he/she may refuse to certify until/unless issues (**NC**s in particular) are resolved.