Smarten-up your ISO 27001 SoA with custom controls

Gary Hinson Gary@isect.com

August 2025

Summary

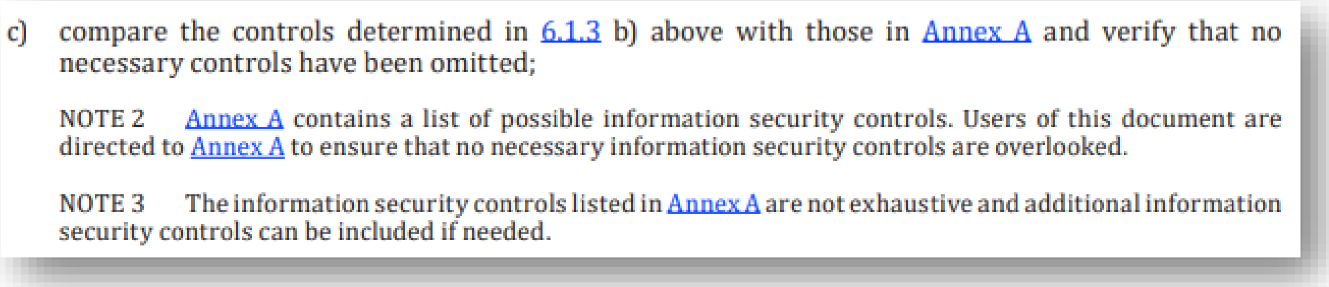
ISO/IEC 27001 implementation and certification are complicated by subjective interpretations of the ambiguously-worded Annex A controls. Rather than naïvely adopting the standard's vague and incomplete checklist of generic controls, a better strategy is to adopt a set of carefully-phrased **custom controls** linked to the organisation's particular risks. This shifts management's focus from mere conformity to the suitability and adequacy of the chosen security measures. The business-focused and risk-aligned approach described here delivers information security that truly satisfies the organisation's needs.

Context

Organisations seeking to adopt and be certified against ISO/IEC 27001 must decide which information security controls are to be managed through their **I**nformation **S**ecurity **M**anagement **S**ystem. The first couple of points under '27001 clause 6.1.3 require the definition and use of an information security risk treatment process to "select appropriate information security risk treatment options, taking account of the risk assessment results" (meaning the information security risk assessment process defined in the previous clause) and "determine all controls that are necessary to implement the information security risk treatment option(s) chosen" – designing controls as required or identifying them from any source.

So far, so good – right? Within the scope of the ISMS, management decides how to treat unacceptable information security risks, typically mitigating them with suitable information security controls.

However, things become confusing when we get to clause 6.1.3 (c):



c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

How do *you* interpret that ambiguously-worded clause? Either:

- The "possible information security controls" in Annex A are, in fact, necessary (but may not be sufficient);

… or …

- Annex A is just a checklist to catch any commonplace controls that have been overlooked.

Checklist
Succinct list of things to do or items to check-off
Cybersecurity Hyperglossary

While the first interpretation is simpler, it conflicts with the earlier requirement that necessary controls are determined by the organisation, not by the standard. Therefore, the correct interpretation is that Annex A is a reminder, *not* a list of necessary controls. To put that another way:

the Annex A controls are discretionary, *not* mandatory for certification.

The problem with Annex A controls

If an organisation states in its **S**tatement **o**f **A**pplicability that an Annex A control is necessary, the certification auditors are at liberty to confirm whether the control is being managed in accordance with an ISMS that fulfils the standard's main-body clauses. That begs questions such as:

1. Does the control adequately mitigate the information security risks as it was supposed to do? What are those risks, in fact? Has the control been justifiably selected?
2. Is the control substantially as stated in Annex A?

Question 1 involves subjective determinations such as which information risks the control was intended to mitigate and whether it brings the risk within management's risk appetite. Since the standard does not address either point, auditing them can be tricky. In contrast, question 2 is fairly straightforward for a conformity auditor to test objectively. Take control A.5.1 for instance:

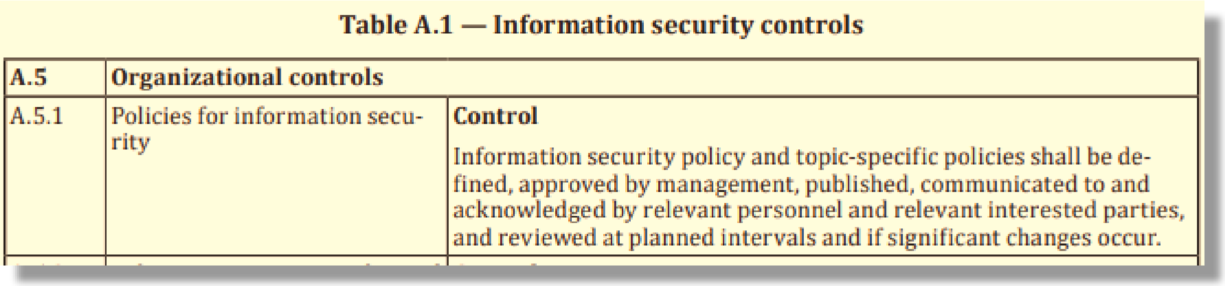


Table A.1 — Information security controls

A.5	**Organizational controls**	
A.5.1	Policies for information security	**Control** Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

As worded, the control requires that the information security policy and topic-specific policies are:

1. Defined;
2. Approved by management;
3. Published;
4. Communicated to relevant personnel and interested parties;
5. Acknowledged by relevant personnel and interested parties;
6. Reviewed at planned intervals; [and]
7. Reviewed if significant changes occur.

While none of those requirements is crystal-clear (*e.g.* what does it mean, exactly, to 'define' a policy? What are 'planned intervals'?), the auditor can simply ask for copies of the policies to check against the seven points *e.g.* are the policies documented (implying 'defined' and 'published')? Were they formally signed-off by management (indicating approval)?

Inability to demonstrate any of the seven points suggests that the organisation does not conform to its own SoA, meaning that the ISMS fails to satisfy clause 4.4. The issue then becomes whether the failure is so significant that it blocks certification. Significance or materiality requires yet another subjective determination by the auditor.

All the 'necessary' controls are potentially liable to be audited in a similar manner – or not: the auditor decides how much audit testing is appropriate ('necessary' you could say!).

In short, the ambiguity in Annex A control wording and the subjectivity in implementation and are problematic. **By stating in its SoA that Annex A controls are 'necessary', an organisation is inviting trouble.** So, is there a better way?

Custom controls, a smarter approach

Yes, there is an alternative approach. Management can select a set of **custom controls** for the SoA that are worded more definitively and precisely than Annex A.

For example, in place of A.5.1, management might specify a custom control that simply and directly states 'Our information security policies are made available on the corporate intranet'. Provided there is indeed evidence that the policies exist on the corporate intranet, they can legitimately claim and demonstrate conformity with their SoA. They might still decide to perform the other actions mentioned in Annex A but would not be formally required to do so. The pressure's off.

Furthermore, if the organisation retains evidence concerning their selection and wording of the custom controls (such as a risk-control matrix, with notes showing that management reviewed and approved it), this supports their assertion that the ISMS conforms to the standard's mandatory main-body clauses.

The organisation should also be prepared to demonstrate (as per 6.1.3(c) note 2) that they have duly considered all the Annex A controls, ensuring that 'no necessary information security controls were overlooked'. This could be a succinct, formal statement from management to that effect in the SoA ("Having reviewed and determined that *none* of the Annex A controls are entirely appropriate as worded, management has determined that the following custom controls are necessary to mitigate unacceptable information security risks:"). A printout of Annex A with notes demonstrating the review, or a cross-reference between the SoA and Annex A, would add more weight if required.

Conclusion

With the custom control approach, ISO/IEC 27001 implementation and conformity assessment naturally focuses on the organisation's information risks and the adequacy of the custom controls intended to mitigate them, rather than the ambiguous wording of Annex A. It is both business-focused and risk-aligned. As such, it is more likely to result in information security that truly suits the organisation.

In short, security trumps conformity.