Documentation and records required for ISO/IEC 27001 certification

April 2016 Release 1

Introduction

We are often asked on the ISO27k Forum what documentation (or "documented information" in the stilted language of the ISO standards) is *formally and strictly required* in order for an organization's Information Security Management System (ISMS) to be certified compliant with ISO/IEC 27001:2013. You'd have thought the answer was simply a matter of checking the standard … but no, it's not quite that easy so we have compiled this checklist to *try* to put this issue to bed.

The checklist identifies in red documentation and records that we believe are *explicitly required* in the main body of ISO/IEC 27001 (they are **mandatory**), plus **additional** documentation, records or other forms of evidence that are implied or hinted-at, including all those identified in Annex A. *In most cases, we identify several possible forms of documentation since there are various ways to fulfil the formal requirements. You do not need them all!* This is patently a detailed checklist. Certification auditors are unlikely to demand *everything* on the list but they will probably want to see:

- *Most* of the **mandatory** things such as your information risk and security policies and procedures;
- *Some* of the records arising from or generated by the processes, such as entries in your risk register, completed corrective/preventive action forms, and metrics;
- Other documentary evidence demonstrating that the ISMS itself, plus the information security controls and other risk treatments are in effect, such as ISMS internal audit reports and perhaps security designs, configuration details, patching records, insurance policies *etc*.

Implementation tip: the auditors will expect to choose their own samples for review. You can't simply pick out and present the few items that you know are good and bury the rest! To demonstrate your professionalism, impress the auditors, and make the audit as painless as possible, prepare for the audit by sorting, filing and referencing/indexing the documentation, chasing down any missing pieces, weeding out irrelevant/older content *etc*. This should be a routine ISMS housekeeping activity anyway.

There is further guidance in clause 7.5 of the standard, and there are several document samples/templates in the free ISO27k Toolkit.

About Annex A

For certification purposes, the formal status of ISO/IEC 27001 Annex A, and hence of the requirements scattered throughout it, is decidedly ambiguous[1]. Your **Statement of Applicability** (SoA) may conceivably declare virtually all of the controls in Annex A unnecessary or inappropriate to your business situation, in which case obviously hardly any of the corresponding Annex A requirements are applicable or mandatory to your organization. However, should you seek certification, not only will you need to document and explain *why* those controls are inapplicable, but the auditor may vehemently disagree and refuse to certify you if there are controls whose absence patently fails to address information risks that are significant for the organization. For example, you may feel there is no need for controls against malware if your organization only uses cloud-based IT services through dumb terminals running simple web browsers; however, the certification auditor will raise the red flag if the information assets within the scope of the ISMS are, in fact, vulnerable to malware yet the malware controls are lacking or inadequate, having been declared inapplicable. [That's an extreme and rather unlikely situation: in practice, there are more than 50 shades of grey here.]

On the other hand, you are free to choose other risk treatments or controls, aside from or in addition to those recommended in Annex A. Most of them will involve documentation, so there's no getting away from it! Regardless of how it is expressed, your organization undoubtedly *needs* numerous information security controls to mitigate its information risks, and the certification auditors will expect to be convinced that management has a firm grip on them through the ISMS as a result of reviewing the documentary evidence. Hard-liners may even insist that 'if something is not documented, it doesn't exist'.

> "If you do it, document it. Treat documentation of all process and standards as mandatory."
>
> *Walt Williams*

Other documentation guidance

Aside from ISO/IEC 27001 itself, we recommend ISO/IEC 27006 (certification) and ISO/IEC 27007 (management systems auditing) since the certification auditors will be using them both to review and hopefully certify your ISMS. ISO/IEC 27002 is invaluable because it expands significantly on ISO/IEC 27001 Annex A, while ISO/IEC 27005 plus ISO 31000 cover risk management. For business continuity management, ISO 22301 does a *much* better job than ISO/IEC 27001 section A17. When released (hopefully in 2016), the *next* versions of ISO/IEC 27003 (ISMS

[1] In the notes to section 6.1.3 (c), Annex A is described as a comprehensive [yet] non-exhaustive list of control objectives and controls. Which is it? It can't be both! Also, the note to 6.1.3 (b) says "Organizations can design controls as required, or identify them from any source" in contradiction to 6.1.3 (c) and (d) which strongly imply that Annex A is mandatory. Furthermore, Annex A is described as "Normative", again implying that it is mandatory. However, you may choose to implement controls from COBIT, NIST, PCI-DSS, FedRamp, HIPAA, CSA STAR *etc*. instead of or in addition to the controls listed in Annex A without affecting your organizations' ability to be certified compliant with ISO/IEC 27001. In the same vein, industry-specific variants of ISO/IEC 27002 provide 'extended control sets' that are thought to be especially relevant to certain industries – currently telecoms (ISO/IEC 27011), finance (27015) and health (27799).

implementation) and ISO/IEC 27004 (measurement and metrics) should be much more useful than the current standards, but some may find value in those too. There are many other information risk, information security and management systems standards, advisories and books as well, while various laws, regulations, contracts, agreements, industry norms and stakeholder expectations may impose further obligations or constraints on your documentation and ISMS (as noted in section A18.1).

However, *this* checklist is solely concerned with the generic documentation requirements and recommendations of ISO/IEC 27001.

Implementation tip: bear in mind that **being certified is not the ultimate goal**. It is even more important that your ISMS (whether certified or not) suits the needs of the organization and earns its keep, long term. It is *easy* to become completely consumed with the certification process, introducing layers of complexity and red tape that are costly, counterproductive and of no real value to the business. Resist the urge by remaining pragmatic. There will be plenty of time to elaborate on and enhance things afterwards, if that is appropriate. Such changes are exactly the kinds of things that management systems are intended to manage, systematically, as your ISMS matures.

You may need more … or less!

Your ISMS *may* need still more documentation - beyond both the **mandatory** and **additional** requirements noted in this checklist … and that's absolutely fine: ISO/IEC 27001, ISO/IEC 27002 and BS 7799 before them were never intended to be totally comprehensive or prescriptive.

Your ISMS may use different documentation in various areas. The auditors will take a lot of convincing if your **mandatory** documentation varies *substantially* from that described in the standard, but you can expect more latitude and flexibility with the **additional** materials.

Any operational ISMS will also generate quite a variety of **records** *i.e*. the outputs of various processes/activities. We've given lots of examples in the checklist, but you may have only some of these or alternatives.

Implementation tip: if this is your first attempt to be certified compliant with ISO/IEC 27001, be realistic about the amount of documentation and records you can reasonably specify, create, approve, use, manage and maintain, and the costs of all that red tape. We strongly suggest keeping it down to the minimum for now with the option to expand it later as your certified ISMS matures, you gain experience and your confidence grows stronger. Retain records for as long as you might need to refer back to them, preferably neatly filed in sufficient number that the auditors can sample and check a reasonable quantity if they so choose – but don't go overboard. Piling everything up 'forever' in an enormous heap is unnecessary, unhelpful and ultimately unsustainable.

Form and control of ISMS documents

The titles, styles and formats of ISMS-related documentation often vary in practice (*e.g*. purely online/electronic or printed/paper documents, spreadsheets, lists, databases, formal meeting reports and minutes or rough notes, raw measurement data and metrics reports) and there may

be several items of one type (*e.g*. risk assessment reports for different situations, IT systems *etc*.). Go with whatever suits the needs of your ISMS, just so long as the certification auditors are able to review and assess the documentation against the formal requirements. The purpose, contents, and control over them, are more important than their form (within reason!).

Implementation tip: neat diagrams are a good way to summarize or document systems, procedures and information flows clearly and succinctly, and help design, use and manage them in practice. However, there is merit in a standardized format for ISMS documentation, so consider developing and using suitable templates and styles. A reasonably consistent look-and-feel helps 'brand' all the elements together into a coherent and impressive body of work – a management system – with advantages for security awareness, readability and compliance, plus auditing.

Although it does not formally demand as much, ISO/IEC 27001 **clause 7.5** clearly *implies* the need for a well-designed, structured, populated, controlled, managed and maintained *suite* of ISMS documentation. It talks, for instance, about having standard document information (such as title, date, author and reference), review and approval activities, version controls, appropriate access rights and distribution, and so on. BS 5750 and ISO 9001 set the scene, way back. You may decide to manage a small suite of ISMS documentation manually using minimal processes and controls, or for a larger setup adopt a *document management system*, or take some other approach (perhaps mirroring the way your organization manages other similar suites of documentation around safety, finance, people, environment or whatever). Read through and think carefully about clause 7.5. Discuss your options with management as there may be substantial implications on the complexity, scope, costs, timescales *etc*. for your ISMS. Within reason, simpler approaches are almost always better in the long run. It's easier and cheaper to keep fewer things in order, *especially* if you happen to be in a highly dynamic and complex business situation. Most auditors prefer quality over quantity.

A few items crop up more than once in the checklist where they serve multiple purposes. They need only exist once, so long as they are cited/referenced from wherever they are needed – talking of which, you might find it helpful to adopt a standard form of unique naming or numbering for your ISMS documentation, and to keep all the definitive materials in one specific well-controlled place such as a network directory, intranet area, document management system or filing drawer.

Purpose of this checklist

The checklist is designed to be used prior to an internal audit or a certification audit to confirm that everything is in order, and to collate the documentation ready for the auditors to review. Aside from certification, it may also be helpful for gap analyses, internal audits and management reviews of the ISMS. It can be used up-front when planning the ISMS as a guide to the documentation that will have to be created and produced in the course of the implementation project. Consider it a template, a starting point for you to adapt or customize as you wish (within the license terms, anyway) but be very careful not to lose or (further) corrupt any of the **mandatory** documentation requirements in the process!

In the first column, we have *referenced* the relevant clauses of the ISO/IEC standards to make it simple to check the details. **You should be very familiar with the ISO27k standards by the time certification comes around.** The wording here is paraphrased and shortened for copyright and readability reasons, but the ISO/IEC 27001 clause numbering is retained. **Read the standard to discover *exactly* what is required!**

The *Status* column has check boxes for the three typical stages in the preparation of a document: you may want additional boxes (*e.g*. "Allocated", "Approved", "Published" *etc*.) and there will often be several actual documents, but don't *over*complicate things. Remember the ultimate goal is to secure information and support/enable the business, not to pass the certification audit, generate red-tape or incur unnecessary costs. If you can get by with a single "done" checkbox, or live without this column altogether, then please do.

The *Interpretation* column contains our informal, opinionated and at times cynical paraphrasing and explanation of the requirement, as we understand it. We've *tried* to be helpful and pragmatic here. You, your colleagues and the auditors may disagree, and fair enough: at the end of the day, the published ISO27k standards (warts and all) are definitive - not us, you or them.

The *Notes* column is a place to scribble comment and reference the evidence so that you can pull it straight out of the neatly indexed review, audit or gap analysis file on demand. Empty cells in this column, plus a distinct lack of ticks in the status column, suggest that the documentation is incomplete in this area – in which case be ready to explain why, or fix it.

Authorship and copyright

This document was produced by a team of elves from the ISO27k Forum *i.e*. Gary Hinson, Richard Regalado, Ed Hodgson, Walt Williams, Joel Cort and Khawaja Faisal Javed. We *think* it is reasonably complete and fairly accurate (roughly right) but we don't entirely agree among ourselves and it could easily be materially wrong in parts, so it comes with no guarantee: it's up to you to check it (and by all means put us completely right).

Requirement	Status	Interpretation	Notes
		***Mandatory* documentation and records**	
4.3 ISMS Scope	☐ Specified ☐ In draft ☐ Done	The **ISMS scope** clarifies the boundaries of the certified ISMS in relation to the context or business situation of the organization (*e.g.* certain business units, sites or departments), and its information risks and security requirements plus any imposed by third parties (*e.g.* laws and regulations plus contractual obligations and often, in a group structure, strategies and policies mandated/imposed by HQ). Security must be taken into account whenever information crosses scope boundaries. A high-level business-driven **strategy** or **vision statement** (either made or at least formally endorsed/signed-off by senior management) is one way to crystallize both the scope and purpose of the ISMS, and can be useful for awareness/promotional purposes too.	
5.2 Information security policy	☐ Specified ☐ In draft ☐ Done	The **information security policy** (or policies) lays out and confirm senior management's commitment to (a) the organization's information security objectives and (b) continuous improvement of the ISMS … and often much more. Senior management may prefer to mandate a single, succinct, broad/overarching governance-type policy (formally satisfying the ISO requirement), supported by a suite of detailed information risk, security, compliance, privacy and other policies, procedures, guidelines *etc.* (see A5.1.1) or you may take a different approach.	
6.1.2 Information security risk assessment Process documentation	☐ Specified ☐ In draft ☐ Done	It is up to you to determine precisely what is appropriate for your organization using clause 6.1.2 as a guideline plus ISO/IEC 27005 and ISO 31000. The auditors expect a structured and repeatable process *i.e.* a documented **risk assessment procedure** explaining how you identify, analyze (e.g. identify potential consequences and probabilities of occurrence), evaluate (*e.g.* use specified **criteria for risk acceptance**) and prioritize your information risks (e.g. using risk levels), with **periodic reviews/updates** to reflect gradual changes plus ***ad hoc* reviews/updates** in response to step-changes in your information risks. You should also make available relevant **reports, entries in your risk register** with **risk**	

Requirement	Status	Interpretation	Notes
		descriptions, identified risk owners *etc*. and **metrics** to demonstrate its operation.	
6.1.3 Information security risk treatment (d) Statement of Applicability	☐ Specified ☐ In draft ☐ Done	The **Statement of Applicability (SoA)** lays out the information risk and security controls that are relevant and applicable to your organization's ISMS, as determined by your risk assessments or as required by laws, regulations or good practice. Cross-reference them against the controls recommended in ISO/IEC 27001 Annex A and ISO/IEDC 27002, plus any alternative/supplementary sources such as NIST SP800-53, ISO 31000, ISO/IEC 20000, ISO 22301 and 22313, IT-Grundschutz, the ISF Standard of Good Practice, assorted privacy laws and principles *etc*. Clarify whether the controls recommended in ISO/IEC 27001 Annex A are in scope and appropriate to your organization, if not providing reasoned justifications (*e.g*. strategic management decisions, formally recorded) to convince the auditors that you haven't simply neglected, ignored or arbitrarily excluded them.	
6.1.3 Information security risk treatment Risk treatment process	☐ Specified ☐ In draft ☐ Done	Again it is up to you to determine precisely what is appropriate for your organization, using clause 6.1.3 plus guidance from ISO/IEC 27005 and ISO 31000. Risk treatment decisions (*e.g.* selecting treatments including applicable controls) and the actions arising (*e.g*. implementing the controls or sharing risks) may be an integral part of the risk assessment process, or a distinct activity or phase. It could be a dedicated activity for information risk, or an integral part of enterprise risk management *etc*. Typical evidence includes a written **policy and/or procedure** for consistently deciding on and implementing appropriate information risk treatments. Convince the auditors that the process is operating correctly by providing relevant **reports, your Risk Treatment Plan, entries in your risk register, metrics *etc***. You may prefer some sort of list, matrix or database structure, a program or project plan, or something else to explain the process through which information risks are being or to be controlled	
6.2 Information security	☐ Specified ☐ In draft	The ISO requirement to "retain documented information on the information security objectives" is vague too, so once more you have some latitude. A good	

Requirement	Status	Interpretation	Notes
objectives and plans	☐ Done	approach is to start with the organization's high level business objectives, deriving information risk and security objectives from them. These can be supported by lower level control objectives and controls and metrics (6.2b).	
7.2 Competence	☐ Specified ☐ In draft ☐ Done	You know the drill: interpret the vague requirement to "retain documented information as evidence of competence" as you see fit – for example, you may rely on **HR records** documenting the relevant experience, skills, qualifications, training courses *etc*. just for the core ISMS people within your information risk and security management function, or extend the net to include *all* the information risk, security, governance, privacy, business continuity and compliance-related people (and possibly others such as security awareness and training professionals, departmental information security/privacy reps, business/security analysts, penetration testers *etc*., perhaps even consultants, contractors and advisors). In time you might develop a **skills matrix** (relating people to rôles according to their skill sets *etc*.), maybe even a **RASCI table** (showing, for each key information risk and security-related process or decision, which functions, rôles or people are Responsible, Accountable, Supportive, Consulted or Informed). We recommend keeping it simple, for certification purposes. You can always do more later on.	
8.1 Operational planning and control Procedures	☐ Specified ☐ In draft ☐ Done	Make what you will of the requirement to "keep documented information to the extent necessary to have confidence that the processes have been carried out as planned". Generally speaking, this implies **management information** concerning the ISMS such as **budgets** and **headcounts** and **progress reports** containing relevant **metrics,** information risk and security **strategies, plans, policies, procedures** and **guidelines**, plus related **compliance activities** to check/measure, enforce and reinforce compliance, plus **records** generated by or information arising from the procedures/activities, and other stuff such as post incident reports, security test reports, security product evaluations, vulnerability assessments, business impact assessments, preventive or corrective actions, security architectures and designs … much of which we have already noted or is	

Requirement	Status	Interpretation	Notes
		covered under Annex A. Although the details will vary between organizations, it should be plainly evident (painfully obvious!) from the documentation that the ISMS is in normal operation, business-as-usual. Simply convince the certification auditors that the ISMS is operating sweetly.	
8.2 Risk assessment results	☐ Specified ☐ In draft ☐ Done	Information should be generated routinely by the risk assessment process noted in section 6.1.2. Examples include **risk assessment reports, risk metrics, prioritized lists of risks, information risk inventories or catalogs** or information risk entries in corporate risk inventories/catalogs *etc*. You may have meeting notices/invitations, minutes of meetings, risk workshop reports, rough notes from discussions arising, formal memoranda, emails expressing concerns about certain risks, or whatever. Again, collate sufficient material evidence to reassure the auditors that the process is generating useful outputs about information risks.	
8.3 Risk treatment results	☐ Specified ☐ In draft ☐ Done	How are you going to prove that identified information risks are being 'treated' in accordance with the process and decisions made? Your **Risk Treatment Plan** might usefully reference evidence/records confirming that risks have been and are being duly treated, such as **control test reports**, **penetration test reports**, **control implementation project plans** plus milestones and closure documents, purchasing and financial records for **capital expenditure**, **metrics** showing a reduction in the frequency and/or severity of the corresponding incidents *etc*., **management review and audit reports**, emails from management congratulating the ISMS team and awarding large bonuses *etc*. Particularly where substantial risks are accepted (including residual risks), there should be evidence such as **signatures of the relevant risk or asset owners** formally acknowledging that (thereby accepting accountability for any incidents arising!).	
9.1 Metrics	☐ Specified ☐ In draft ☐ Done	The ISMS generates various metrics that are used to monitor and drive information risks, controls and the ISMS itself in the intended direction. Evidence here includes **security metrics** in reports, systems, dashboards, presentations *etc*., plus proof that the metrics are being duly noted and acted upon *e.g*. memos, emails or rough notes expressing concern about adverse trends or thanks for	

Requirement	Status	Interpretation	Notes
		positive trends; comments scribbled on printed reports; action plans; minutes of meetings *etc*.	
9.2 ISMS internal audits	☐ Specified ☐ In draft ☐ Done	**ISMS internal audit reports** are the obvious evidence here, documenting the main audit findings, conclusions and recommendations, often in the form of Nonconformity/Corrective Action Reports. Supporting evidence may include audit programs or plans or calendars, budgets and auditor man-day allocations, audit scopes, audit working paper files with detailed audit findings and evidence (such as completed checklists), audit recommendations, agreed action plans and closure notes *etc*. The certification auditors *may* want to interview/chat to the ISMS auditors about the ISMS and/or issues raised in their reports.	
9.3 ISMS management reviews	☐ Specified ☐ In draft ☐ Done	**ISMS management review reports,** obviously, perhaps also calendars/plans, budgets, scopes, working papers with evidence, recommendations, action plans, closure notes *etc*. The certification auditors *may* want to interview/chat to relevant Top Management and managers about the ISMS and/or issues raised in their reports.	
10.1 Nonconformities and corrective actions	☐ Specified ☐ In draft ☐ Done	'Nonconformities' are (partially or wholly) unsatisfied requirements, including those within ISO/IEC 27001, plus strategies, policies, procedures, guidelines, laws, regulations and contracts. They may be documented in the form of issues, events, incidents, audit and review findings, complaints, or simply as "nonconformities" (*e.g.* on a Nonconformity/Corrective Action Report NCAR form). The certification auditors need to be convinced that nonconformities are being routinely and systematically identified, raised/reported, addressed and resolved, by reviewing (their sample of) relevant documentary evidence. Make it easier for them by maintaining a **register or index of nonconformities**, along with the neatly-filed evidence of actions undertaken in response to the nonconformities such as: root-cause analysis; reaction to the nonconformity such as immediate containment or correction; final results of the corrective action including review of its effectiveness and completion/closure/sign-off for the nonconformity.	

Requirement	Status	Interpretation	Notes
Additional documentation, records and evidence			
Main body of ISO/IEC 27001			
4.1 Organization and context	☐ Specified ☐ In draft ☐ Done	Identify yourself. Use a diagram and show an organizational chart as to where your team and operation resides and who are the Top Management stake holders. Represent both the technical team and the business team The documented process or procedure of holding a **strategy meeting** (or similar) where internal and external issues relevant to the ISMS are discussed. Minutes of a **strategy meeting** (or similar) where management discussed various internal and external issues that were relevant to the ISMS – preferably within the past year. While the minutes will provide evidence of the process being followed, the process itself should be documented.	
4.2 Interested parties	☐ Specified ☐ In draft ☐ Done	Some sort of **list of stakeholders** in the ISMS, updated periodically (implying a procedure to formulate and maintain the list). This may include or reference lists of laws, regulations, contracts, agreements *etc*. that are relevant *i.e*. concern risks to and requirements for the security/protection/control of information. Internal corporate stakeholders in the ISMS should also be identified, including not just those who direct and oversee the ISMS but also those who depend on its correct operation ('customers' of the ISMS).	
4.4 ISMS	☐ Specified ☐ In draft ☐ Done	Your **ISO/IEC 27001 compliance certificate** from an accredited auditor is or will be the ultimate evidence of this! Meanwhile, your ISMS has a raft of documented policies, procedures, guidelines *etc*. These are best kept in order, under control and available to all who need them, for example on an **intranet site, Document Management System or Governance Risk Compliance system**.	
5.1 Leadership	☐ Specified ☐ In draft ☐ Done	Evidence of management commitment to the ISMS may include their obvious interest and active involvement in the certification audit and other important ISMS activities (*e.g*. risk workshops), adequate **budgets**, **approval** of various formal documents (including budgets, expenditure and overspend/contingency),	

Requirement	Status	Interpretation	Notes
		explicit reference to information risk and security in **strategies and plans** *etc*. **Communications** from senior management to all staff are excellent evidence (see also 7.4 below), for example when the certification efforts are launched (announcing the strategy, explaining key targets, stating who leads the effort and directing everyone to support the ISMS). Further communications should be issued for example about the certification audits, award of the certificate *etc*., reinforcing the ongoing efforts to use, maintain and improve the ISMS. The seniority level or rank of the most senior information risk and security person (*e.g*. CISO or ISM), and the breadth of scope of the ISMS, are also strong indications of how seriously management takes this.	
5.3 Rôles and responsibilities	☐ Specified ☐ In draft ☐ Done	The level or rank of the most senior information risk and security person (*e.g*. CISO or ISM) relative to other departments/functions, and the breadth of scope of the ISMS (*e.g*. buried within IT, limited to specific business units or organization-wide), are strong indications of how seriously management takes this. The governance arrangements are generally documented in **organization charts** showing reporting lines, **rôle/job descriptions**, **vacancy notices** *etc*.	
6.1.1 Actions to address risks and opportunities	☐ Specified ☐ In draft ☐ Done	This is a high-level requirement that the ISMS helps the organization manage its information risks and security controls systematically, on an ongoing basis. Evidence may include **strategy documents**, **vision statements**, minutes of **ISMS management meetings**, **corrective actions** Done, management and audit **recommendations** actioned, improving **metrics** *etc*. In time, the continued success of the ISMS should speak for itself.	
7.1 Resources	☐ Specified ☐ In draft ☐ Done	ISMS resources are primarily people (**Full Time Equivalents**, **headcount** or **list** of permanent employees plus consultants, contractors, advisors, interns, temps *etc*.) and **budgets**. Note that the true expenses/costs of information risk and security, and the benefits, are distributed widely throughout the organization across all the activities that involve information: however, it is much simpler (and usually sufficient) to account purely for the Information Risk and Security	

Requirement	Status	Interpretation	Notes
		Management function operating and managing the ISMS. Talk to your finance department about which accounting codes and reports to use.	
7.3 Awareness	☐ Specified ☐ In draft ☐ Done	Evidence for the security awareness activities includes any relevant procedures and standards, **awareness materials** (posters, presentations, briefings, web pages, leaflets, quizzes, competitions, training course notes, lists of rewards/prizes issued *etc*.) and **metrics** (*e.g.* records of attendance and feedback scores from awareness events, awareness survey and test results, and details of the ongoing investments in security awareness and training).	
7.4 Communication	☐ Specified ☐ In draft ☐ Done	The requirement is *very* vague here. Think about what you communicate regarding the ISMS, to whom, when and how, and gather relevant evidence about it – emails, notices, reports, metrics *etc*. Document the internal communications processes as well as collect evidence that shows them in operation.	
7.5.1 General documentation	☐ Specified ☐ In draft ☐ Done	**This very checklist**, once completed and supported by the referenced documentation and records, is a simple way to demonstrate to the auditors the nature, breadth, volume and quality of information concerning and generated by your ISMS. In addition to using this as part of your preparation for certification, you might like to maintain it indefinitely as a living record of your ISMS documentation, or perhaps migrate everything to a Document Management System with the functionality to track and report on all the documentation. ISMS documents need to be reviewed and updated periodically, with the reviews, changes and re-authorization being noted within in the documents themselves and/or in the DMS.	*This doc!*
7.5.2 Creating and updating docs	☐ Specified ☐ In draft ☐ Done	A set of **document templates** for all the ISMS documents is a simple way to make sure they all have the standard document or version control information (such as the revision history, and any authorizations or mandates), as well as making them more consistent.	
7.5.3 Control of docs	☐ Specified ☐ In draft ☐ Done	Document management systems and webservers can generate reports of **access rights**, document **status** *etc*. for policies, procedures and guidelines *etc*. Emails, management reports, review and audit reports, metrics reports *etc*. generally	

Requirement	Status	Interpretation	Notes
		state their own distribution on the cover, or may use **classification** rules or managed **distribution lists**.	
10.2 Continual improvement	☐ Specified ☐ In draft ☐ Done	Documentary evidence for continual improvement of the ISMS includes the reports of **reviews, audits, incidents, corrective actions, ISMS strategy/planning and management meetings** plus assorted **metrics** demonstrating positive trends (hopefully!).	
Annex A - Further guidance on these controls is provided in ISO/IEC 27002:2013 and other standards			
A.5.1.1 Information security policies **A.5.1.2 Review the policies** **A.6.2.1 Mobile device policy** **A.6.2.2 Teleworking**	☐ Specified ☐ In draft ☐ Done	In addition to the main information security policy (5.2), the organization is expected to have **written policies addressing specific areas of information security**. Examples (*not* a mandatory list) are provided in ISO 27002:2013 clause 5.1.1, and 6.2.1. These need not be separate documents and may include pre-existing policies, for example a data protection or privacy policy. Evidence of policy reviews can be a simple **diary showing the reviews and/or review and approval dates on the policies themselves** (standard document control information). There should be written information security **policies for portable/mobile ICT devices** including personal devices used to access, process or store business information (**BYOD**), plus **teleworking**.	
A.6.1.1 Information security roles and responsibilities **A.6.1.2 Segregation of duties** **A.7.1.2 Terms and conditions of employment**	☐ Specified ☐ In draft ☐ Done	Information risk and security rôles and responsibilities are normally documented in **job descriptions, vacancy notices, policies, employee handbooks, contracts of employment, service contracts** *etc*., particularly for the 'obvious' jobs such as CISOs, Information Security Managers and Security Guards. Another/complementary approach is to draw up a **matrix** with jobs/rôles on one axis and responsibilities on the other, or a **RASCI chart** (there's a template in the ISO27 Toolkit). Mutually exclusive rôles should be identified as such (*e.g.* separating the definition, implementation, allocation and review/audit of access rights for important IT systems). Depending on the situation, don't forget about contractors, consultants, temps, interns, facilities/maintenance workers,	

Requirement	Status	Interpretation	Notes
		home workers and (perhaps) privileged vendor support people working on company business on- or off-site [your organization may specify information security requirements in contracts with the vendors, who in turn may specify information security rôles and responsibilities in their employment contracts].	
A.6.1.3 Contact with authorities **A.6.1.4 Contact with SIGs**	☐ Specified ☐ In draft ☐ Done	**Contact details, business cards, membership certificates, diaries of meetings** *etc*. can provide evidence of professional contacts, particularly for information risk, security and compliance specialists. Is anyone in touch with CERT, professional bodies such as ISACA, $(ISC)^2$ and ISSA, industry regulators *etc*.? Prove it! Valid contact details embedded within incident response, business continuity and disaster recovery plans is further evidence of this control, along with notes or reports from previous incidents concerning the contacts made.	
A.6.1.5 Infosec in projects	☐ Specified ☐ In draft ☐ Done	**Project management manuals, methods, policies, procedures, guidelines, forms** *etc*. should include relevant information risk and security activities.	
A.7.1.1 Screening	☐ Specified ☐ In draft ☐ Done	Records of **identity and background checks** are normally maintained by HR, Security *etc*. as part of employees' personnel info. The checks may be done routinely prior to employment (*e.g.* checking/copying passports or other official photo-ID at interview), periodically for trusted rôles, on promotion into such rôles, when personnel incidents occur/concerns are raised, and perhaps randomly as a deterrent. Don't forget about contractors, consultants, interns, advisors, temps *etc*.	
A.7.2.1 Management responsibilities	☐ Specified ☐ In draft ☐ Done	A formal **management statement to employees** mandating their compliance with the information security policies and procedures. This may go out as an email or memo, be re-stated in the front of the security policy manual and on the intranet site where policies and procedures are made available, and perhaps included and explained in security training and awareness materials.	
A.7.2.2 Security awareness and training	☐ Specified ☐ In draft ☐ Done	Your **security awareness and training materials** should demonstrate that an effective, lively, ongoing awareness program is in operation. Examples: awareness posters, briefings, slide decks for seminars and courses, guidelines,	

Requirement	Status	Interpretation	Notes
		tests and quizzes, plus **metrics** (see 7.3 above). Regular or *ad hoc* awareness updates are required to pick up on changes, emerging risks *etc*. and maintain awareness levels and skills. Professionals/specialists with significant responsibilities in information risk, security, governance, compliance *etc*. may need suitable, in-depth training (*e.g.* PCI-DSS for those handling credit cards, HIPAA for those handling patient information, and privacy laws and regulations for those handing personal information). Keep an **awareness diary** and rolling **plan** and update **employee training records**.	
A.7.2.3 Disciplinary process	☐ Specified ☐ In draft ☐ Done	A formal **disciplinary process** may be part of your HR procedures / staff handbook and cited in employment/service contracts *etc*. **Records of disciplinary actions undertaken** should prove that the process is being followed but may be too confidential to disclose in full, especially for any ongoing disputes or legal cases.	
A.7.3.1 Termination process **A.8.1.4 Return of assets**	☐ Specified ☐ In draft ☐ Done	**Policies, procedures, guidelines and forms supporting the termination process** should incorporate information security elements such as retrieving corporate information and other assets (*e.g.* IT systems, media, paperwork, keys, passes) from them, and explicitly reminding departing employees of their ongoing security, privacy and other obligations, both legal and ethical, towards the organization, its customers, their colleagues *etc*.	
A.8.1.1 Asset inventory **A.8.1.2 Asset owners**	☐ Specified ☐ In draft ☐ Done	An **inventory** (or list or database …) of information assets, IT systems *etc*. including details (names and/or rôles) of their owners, typically managed within IT inventory or management applications.	
A.8.1.3 Acceptable use	☐ Specified ☐ In draft ☐ Done	Typically documented as an **acceptable use policy**, along with **procedures** and other **guidance** *e.g.* a **code of practice** or **employee rulebook**.	
A.8.2.1 Information classification **A.8.2.2 Classification labelling**	☐ Specified ☐ In draft ☐ Done	Typically documented as an **information classification policy**, along with **procedures** and other **guidance** for handling information according to its classification. A selection of duly **marked and protected information assets** demonstrates that the policy is in operation.	

Requirement	Status	Interpretation	Notes
A.8.2.3 Handling of assets			
A.8.3.1 Media management **A.8.3.2 Media disposal** **A.8.3.3 Media transfer**	☐ Specified ☐ In draft ☐ Done	Typically documented in one or more security **policies** supported by **procedures** and **guidelines** concerning portable storage media (USB sticks, portable hard drives, tapes, paperwork *etc*. plus portable devices, briefcases *etc*. *containing* media) - physical access control and protection, encryption, safe storage, labeling, chain of custody records (*e.g.* details and signatures as media are transported by couriers) *etc*. Evidence of **media transport and disposal** may include receipts, confirmations and/or disposal certificates from courier/transport and disposal service providers, whether performed in-house or by competent commercial companies (preferably under **contract**).	
A.9.1.1 Access control policy **A9.1.2 Network access**	☐ Specified ☐ In draft ☐ Done	Typically documented as one or more **access control policies** (possibly one overall policy [supported by something more specific for each major IT system, network or type of information asset such as an **access matrix** showing access permitted by various rôles to various assets, functions *etc*.) along with **procedures for secure logon** and other **guidance** concerning controlled access to information (networks, systems, applications, data, databases, contracts, paperwork, knowledge *etc*.) such as guidelines on passwords, VPNs, firewalls *etc*.	
A9.2.1 User registration **A9.2.2 User access provisioning**	☐ Specified ☐ In draft ☐ Done	Working records from Security Admin typically include Done and actioned **access request forms** plus **authorized signatory lists, logs and reports** from automated access management systems, change authorizations, information exchanged with HR and Procurement (*e.g.* monthly **lists of joiners and leavers**, consultants/contractors, temps) *etc*.	
A9.2.3 Privileged user management **A9.4.4 Use of privileged utilities**	☐ Specified ☐ In draft ☐ Done	Details of **special arrangements to control privileged accounts** (*e.g.* ROOT and auditor accounts) and privileged functions/utilities (*e.g.* system, security and database administration) especially on high-risk systems, firewalls, log management and intrusion detection systems, databases or other valuable/vulnerable information – typically policies, procedures and guidelines	

Requirement	Status	Interpretation	Notes
		with operational records demonstrating that the processes are working properly and that changes to privileged accounts are reviewed and controlled.	
A9.2.4 Password management	☐ Specified ☐ In draft ☐ Done	Policies and procedures for **creating, communicating and changing passwords**, PIN codes, crypto keys, physical keys *etc*. with operational records from Security Admin, access management systems *etc*. demonstrating that the processes are working properly.	
A9.2.5 Access rights reviews **A9.2.6 Access rights adjustment**	☐ Specified ☐ In draft ☐ Done	Policies, procedures and notes or reports arising from periodic/*ad hoc* **reviews, reconciliation** and **re-authorization of access rights** including evidence that inappropriate rights have been identified, considered and addressed (possibly incident or change records).	
A9.3.1 Password security **A9.4.3 Password management**	☐ Specified ☐ In draft ☐ Done	Policies, procedures and guidelines concerning the choice and enforcement of strong **passwords**, password secrecy, password vaults, password changes *etc*.	
A9.4.1 Information access restriction	☐ Specified ☐ In draft ☐ Done	**Procedures** for restricting access to information and applications in line with the classification and handling rules set out in A8.2, plus records of their operation such as **access reports** from IT systems, databases, firewalls *etc*., **change management records** for significant access right changes *etc*.	
A9.4.2 Strong authentication	☐ Specified ☐ In draft ☐ Done	Policies, standards, procedures, technical architectures/designs *etc*. concerning **multi-factor authentication** or similar arrangements to strengthen identification and authentication and access controls for high-risk systems, privileged functions *etc*. *e.g.* procedures for issuing, using, retaining, replacing and recovering security tokens/fobs, digital certificates, access-all-area passes, master keys *etc*.	
A9.4.5 Source code access	☐ Specified ☐ In draft ☐ Done	Policies, procedures, guidelines and evidence concerning controlled access to program source code – typically available from **source code library management** systems.	

Requirement	Status	Interpretation	Notes
A10.1.1 Crypto policy **A10.1.2 Key management**	☐ Specified ☐ In draft ☐ Done	**Cryptography policy, standards, policies and guidelines** concerning algorithms and key lengths for encryption and authentication, key management, PKI (*e.g.* **Certification Practice Statement**), digital certificates, digital signatures *etc*.	
A11.1.1 Physical perimeter **A11.1.2 Physical entry control** **A11.1.3 Secure offices/facilities**	☐ Specified ☐ In draft ☐ Done	Evidence here is plain to see, or conspicuous by its absence! Controls and vulnerabilities can be substantiated through a **physical site inspection** (walk-through or physical penetration test), photographing signs, fences, barriers, locks, chains, turnstiles, gates, emergency exits, loading ramps, guard houses, key cabinets *etc*., plus discussion with Site Security/guards and Facilities Management. Some organizations **regularly inspect** their physical security arrangements, generating review reports, diary entries, incident reports, maintenance logs *etc*. If security guarding is outsourced, **contracts** plus security procedures *etc*. should clarify the expected controls while patrol logs *etc*. plus inspection should confirm that they are operating correctly. Other evidence might include **visitors' books, logs** for access cards or keys issued to contractors, temps, guards, maintenance engineers *etc*.	
A11.1.4 Environmental protection	☐ Specified ☐ In draft ☐ Done	**Maps, weather and news reports, local council records** *etc*. may indicate physical geographical/topological threats to the area containing corporate facilities (*e.g.* flood plains, fault lines, sinkholes/caves, landslips, tornadoes/hurricanes, ice, erosion, major flight paths, highway over-passes or off-ramps, war zones …). Physical inspection and photography provides further evidence.	
A11.1.5 Working in secure areas **A11.1.6 Delivery/loading bays**	☐ Specified ☐ In draft ☐ Done	Policies, procedures, guidelines, notices *etc*. concerning **access to secure zones** (*e.g.* "No lone working" and "Visitors must be accompanied at all times") and **delivery ramps/loading bays/tradesmen's entrances**. Other evidence includes security guard patrol and incident response procedures, CCTV footage, card access system reports, visitor books and records associated with staff and visitor passes, keys *etc*. plus physical inspection and photographs (if permitted!) of the	

Requirement	Status	Interpretation	Notes
		access controls (*e.g.* locks, barriers, slab-to-slab partitions, intruder alarms, fire exits).	
A11.2.1 Equipment **A11.2.2 Supporting utilities** **A11.2.3 Secure cabling**	☐ Specified ☐ In draft ☐ Done	**Site maps, physical inspection and photography** should confirm that IT equipment, storage media, computer facilities, paper files/filing cabinets, archives/store rooms, videoconferencing facilities *etc*. are **sited and stored in adequately secure areas** (*e.g.* with barriers and locks, safes, screens not visible from public land) with **high-grade utilities** (*e.g.* power feeds and distribution, air conditioning) and controls (*e.g.* fuses, monitoring and alarms for intruders, fire/smoke, water and power issues, CCTV, UPS with battery and generator backup) as necessary to provide appropriate environmental protection (A11.1.4).	
A11.2.4 Maintenance	☐ Specified ☐ In draft ☐ Done	Policies, procedures, guidelines and records (such as **installation inspections, maintenance logs, test reports** and **fire certificates**) should confirm that the facilities operations, management, security and maintenance activities are adequate.	
A11.2.5 Removal of assets	☐ Specified ☐ In draft ☐ Done	**Policies, procedures, guidelines and records** should cover rules for and **authorization** of physical removal of IT equipment and storage media from storage or from site *e.g.* portable IT devices, security tokens, keys, tapes and disks, paper files, equipment/media sent for repair or archival. It is possible to reconcile (a sample of) the current **asset removal records** against reality *e.g.* by confirming that they were properly authorized, that the employees are still employed (!) and that they can produce the assets for inspection, and that all valuable information assets can be accounted for: such a **stock-check** should probably be a routine activity, so there should be notes, reports, incident records *etc*.	
A11.2.6 Security of off-site assets **A11.2.8 Unattended equipment**	☐ Specified ☐ In draft ☐ Done	Policies, procedures and guidelines should specify protection of information on smartphones, laptops, tablets, USB sticks, portable hard drives, valuable papers, knowledge workers *etc*. when off-site *e.g.* **home office security**, in vehicles especially **public transport**, when staying at hotels, conferences *etc*., and **working-from-home/teleworking/remote network access** *e.g.* VPNs. Physical	

Requirement	Status	Interpretation	Notes
		and logical controls may be required *e.g.* firesafes, encryption, health and safety. Note: BYOD should be covered similarly to corporate stuff.	
A11.2.7 Secure disposal and re-use	☐ Specified ☐ In draft ☐ Done	Policies, procedures and guidelines for **secure erasure of storage media** or use of strong encryption (with appropriate key management) may include secure **archival** prior to disposal/re-use.	
A11.2.9 Clear desks and screens	☐ Specified ☐ In draft ☐ Done	Compliance with **clear-desk clear-screen policies** can simply be assessed by workplace inspections during or outside normal working hours … which might be routine for the security guards, in which case there should be **reports** and **incident logs**. **Screen-lock** timeouts with password reactivation may be set by Windows domain policies or local configurations – check the approach and records.	
A12.1.1 Operating procedures **A12.1.2 Change management** **A12.1.3 Capacity management**	☐ Specified ☐ In draft ☐ Done	There should be a suitable range of **information risk and security-related procedures** plus the associated policies, guidelines, awareness and training materials, checklists, forms *etc*., all of which should be of good quality, readable, authorized, controlled, disseminated, used (generating **records**) and maintained (yes, this is another prod about the documentation requirement in the main body **section 7.5**). Examples: installation and configuration of IT systems; backups and archives; job scheduling; errors, alarms and alerts, plus logging and monitoring; patching, change management and version control; capacity and performance management.	
A12.1.4 Segregation of dev, test and prod **A14.2.6 Secure dev environment**	☐ Specified ☐ In draft ☐ Done	Policies, procedures and guidelines should clarify how assorted specifications, source code, executables, libraries, system documentation, data, people *etc*. for **IT development, test, production and support environments** are distinguished, kept separate and controlled, including how they are migrated, checked in/out or promoted between them. Records (*e.g.* logs from the software library or version management system, and reports from reviews, reconciliations or audits) should demonstrate that things are working correctly.	
A12.2.1 Antivirus	☐ Specified ☐ In draft	To prove that the organization has designed, implemented, checked, used, managed and maintained suitable **malware controls**, auditors may check policies,	

Requirement	Status	Interpretation	Notes
	☐ Done	procedures, guidelines, architectures/designs, contracts and records (such as details of **malware incidents**, **antivirus program and signature file update histories**, **software installation records**, and **awareness/training records**).	
A12.3.1 Backups	☐ Specified ☐ In draft ☐ Done	Valuable information assets (computer data, paperwork *and* knowledge workers!) should be regularly backed up and stored safely and securely … and must be capable of being restored as and when needed. Evidence may include: **backup strategies, architectures, policies, procedures and guidelines, schedules, backup management systems and associated records, logs, test reports** *etc*. Note: don't forget off-site data (*e.g.* home/mobile workers and cloud) and off-site storage (*e.g.* data and paper archives).	
A12.4.1 Event logs **A12.4.2 Log security** **A12.4.3 Admin and operator logs**	☐ Specified ☐ In draft ☐ Done	Various security-related activities, events and incidents should be routinely recorded in **logs, warnings, alarms, alerts, metrics** *etc*., both as an historical/evidential/forensic record and to trigger follow-up actions such as incident response. There is usually a *very* large volume and variety of information in this category, hence the auditors may only sample-check some, if any. They may be more interested in the overall **strategies** (*e.g.* for log management), **architecture**, systems (*e.g.* **IDS-IPS** and **SIEM**), **policies and procedures**, **information flows** and the associated information security controls protecting the logs, systems and links against accidental damage, equipment failure, 'loss of signal' and deliberate interference/manipulation/fraud (*e.g.* **centralized log management** arrangements with strong access controls, digital signatures, privacy controls, keep-alive/heartbeat timers, covert monitoring, honey-tokens *etc*.).	
A12.4.4 Clock synch	☐ Specified ☐ In draft ☐ Done	The **network/systems architecture** should take account of the need to synchronize or coordinate various system clocks for various reasons including reliable evidence of the exact time of occurrence of incidents and activities (*e.g.* a **policy** on using UTC, with NTP distributed by time servers referenced to atomic clocks). Note: extreme accuracy or precision is seldom as important as time coordination, but in some circumstances it is vital.	

Requirement	Status	Interpretation	Notes
A12.5.1 Software installation **A12.6.2 Restricting software installation**	☐ Specified ☐ In draft ☐ Done	**Software testing, change-approval, version management and implementation records** may suffice in this area, along with the policies and procedures (*e.g.* a library of approved/authorized/whitelisted apps; backups taken both before and after installation; restricted rights to update software). See also A14.2.	
A12.6.1 Technical vulnerability management	☐ Specified ☐ In draft ☐ Done	The basic control is a reasonably comprehensive and accurate **inventory** of systems, vulnerabilities *etc.*, plus the associated policies and procedures to build, maintain, use, manage and control it. There should also be A **policy and procedure** on patching including roles and responsibilities, plus records or logs of events, incidents and/or changes arising (*e.g.* testing and applying security patches urgently), plus notes concerning security patches not applied (with reasoned justifications such as incompatibilities or greater risks arising from patching than from not patching) and metrics. Note: there are several other vulnerabilities too (*e.g.* ignorant or careless employees, dependencies on unreliable 3rd-parties, and badly locater, constructed and maintained buildings) plus threats and impacts together constituting information risks.	
A12.7.1 Systems audit controls	☐ Specified ☐ In draft ☐ Done	Evidence may include **details of audits** scoped, planned and conducted to avoid impacting operational IT services, **audit reports** and technical information about any ongoing system security/audit functions (*e.g.* logging/alarming whenever significant privileges, control bypasses or other such events take place), plus the usual policies and procedures, maybe even strategies and designs.	
A13.1.1 Network security **A13.1.2 Network service security** **A13.1.3 Network segregation**	☐ Specified ☐ In draft ☐ Done	**Network (security) architecture diagrams, strategies, policies and procedures** are the primary documentation in this area, demonstrating the organization's approach to defining and implementing distinct network security domains or zones (*e.g.* WAN-DMZ-LAN, CCTV and card access networks, shop floor/SCADA/ICS networks, 3G and other public or private networks, VOIP). Additional information may provide further details such as types of routers and firewalls, firewall rulesets, VPNs and other layered networks, intranets and	

Requirement	Status	Interpretation	Notes
		extranets, cloud (*aaS), WiFi and other wireless networks, out-of-band signaling/control/administration/logging/alarms, IDS/IPS *etc*. and possibly records concerning the operation of network security alarms, incident response, security administration activities (*e.g.* network security audits, reviews and penetration tests, network change management, network capacity and performance management) and business continuity aspects (*e.g.* resilience, redundancy/diverse routing, fail-over, fallback/recovery).	
A13.2.1 Information exchange **A13.2.2 Transfer agreements** **A13.2.3 Messaging**	☐ Specified ☐ In draft ☐ Done	Security **strategies**, **policies** and **procedures** concerning the **communication** of valuable/sensitive/important information with other parties (*e.g.* Reuters, stock markets, business suppliers, partners and customers, banks and credit-checkers, analysts, insurers, auditors, authorities, peers, CERT), and the associated controls (*e.g.* risk analysis, contracts, addressing, identification and authentication, encryption, logging and alerting, secure couriers, delivery confirmation/receipt for nonrepudiation, check-totals and message counts, keep-alive or heartbeat arrangements with null messages and alerts on link failure, diverse routing, emergency contacts *etc*.).	
A13.2.4 NDAs	☐ Specified ☐ In draft ☐ Done	Discrete **Non-Disclosure Agreements** are the obvious evidence here, but also **confidentiality** clauses embedded in various agreements (*e.g.* consulting, professional advisors and employment contracts), and perhaps the associated **policies, procedures, guidelines** *etc*. detailing the controls to monitor and achieve compliance.	
A14.1.1 System security requirements **A14.1.2 Securing public apps** **A14.1.3 Transaction security**	☐ Specified ☐ In draft ☐ Done	**Strategies, policies, procedures and guidelines** concerning how information risks are identified, assessed and treated in the course (throughout the entire lifecycle) of software/systems development activities (*e.g.* **structured development methods** with documented risk analysis, security design/selection, secure platforms, security services/functions/processes, secure development/coding, security and performance testing, implementation/configuration, post-installation verification, system maintenance and management activities, forms *etc*.) concerning the full breadth of application/system security requirements	

Requirement	Status	Interpretation	Notes
A14.2.1 Secure development **A14.2.5 Security engineering** **A14.2.8 Security testing** **A14.3.1 Securing test data** **A14.2.9 Acceptance testing**		(*e.g.* security engineering, architecture and design, compliance with legal, regulatory, contractual, ethical and commercial obligations/expectation, business process/administrative controls, identification and authentication, access and privacy controls (including specifications, code, test data and test results), crypto, fraud controls, network/messaging security, malware controls, alarms and alerts, logging, security admin, data integrity, backups, resilience and recovery …), and possibly records demonstrating them in action (*e.g.* acceptance or authorization to proceed with implementation), preferably with evidence of a strong business drive and involvement.	
A14.2.2 Change control **A14.2.3 Post-OS update app reviews** **A14.2.4 Restricted changes to packages**	☐ Specified ☐ In draft ☐ Done	Obviously enough, the documentation includes **change control policies, procedures and guidelines**, plus less obviously **change authorization and planning, change logs/records, risk assessments, prioritization and coordination** (*e.g.* change windows, change freezes), back-out plans *etc*. as evidence of their correct operation, even under urgent/emergency/exceptional conditions.	
A14.2.7 Outsourced development	☐ Specified ☐ In draft ☐ Done	**Strategies, policies, procedures** and **guidelines** concerning the (information security aspects of the) use of **3rd-party developers** including contractors, commercial developers and crowd-sourcing/collaborative arrangements *e.g.* contracts and agreements, specifications, standards, monitoring, stage-gate authorizations, acceptance testing, remediation, maintenance and support. [This could potentially include the selection and adoption of commercial, shareware or freeware software packages, modules, libraries, and cloud services/apps *etc*. although that's not strictly what the standard says.]	

Requirement	Status	Interpretation	Notes
A15.1.1 Supplier security **A15.1.2 Supplier agreements** **A15.1.3 Supply chains** **A15.2.1 Service delivery monitoring** **A15.2.2 Changes to 3rd-party services**	☐ Specified ☐ In draft ☐ Done	Documentation in this general area include information security and business continuity **strategies, policies and procedures** concerning **suppliers** and *their* upstream/peer suppliers/partners/customers, plus (potentially) customers and *their* suppliers/partners/customers … depending on the organization's dependence on them and hence the risks. While the standard is primarily concerned with information- or IT- or cloud-related products/goods and services, it also mentions logistics, financial services *etc*. Furthermore, there should be associated records such as **contact points** (for routine operations, and escalation, commercial and exceptional issues), plus **performance and compliance monitoring, incident management, risk assessment and treatment reports, selection criteria, contracts/agreements, reviews, assessments or audits** *etc*. The auditors have limited time and prior knowledge of your situation, so hopefully digging out some of the obvious/key policies and **contracts** will demonstrate willing. Note: supply networks in most organizations are very complex and hence the information (and other) risks and dependencies are very tricky to identify, analyze and treat: remember Sendai! This control extends well into business continuity management, hence BC strategies, policies, arrangements *etc*. are probably partly relevant, as well as broader commercial strategies *etc*.	
A16.1.1 Incident management responsibilities **A16.1.2 Incident reporting** **A16.1.3 Vulnerability reporting**	☐ Specified ☐ In draft ☐ Done	[Information- or IT- or information security-related] **incident management** rôles, **responsibilities and objectives**, plus **policies, procedures and guidelines** (*e.g.* routine and emergency contact points), plus **records/evidence concerning events/incidents** reported, logged, analyzed, possibly escalated, addressed and resolved as evidence of compliance. The auditors will welcome evidence of a managed, measured, systematic, rational and effective process for handling incidents from cradle-to-grave, including **post-incident wash-ups** and substantive organizational changes to embody the learning. For bonus points, show-off your strong forensics capability, and demonstrate that you also discover, respond/react to and learn from near-misses and incidents affecting 3rd-parties.	

Requirement	Status	Interpretation	Notes
A16.1.4 Incident assessment **A16.1.5 Incident response** **A16.1.6 Learning from incidents** **A16.1.7 Forensics**			
A17.1.1 Planning infosec continuity **A17.1.2 Implementing infosec continuity** **A17.1.3 Verifying infosec continuity** **A17.2.1 Availability of ICT services**	☐ Specified ☐ In draft ☐ Done	As literally worded, the standard is primarily concerned with ensuring the continuity of important *information security* activities and controls during a major incident or disaster … but you and I know that information security is generally a relatively minor consideration under such circumstances and is completely trumped by ensuring the continuity of core business activities, hence *sensible* documentation in this area includes **business continuity strategies, policies, plans, procedures, test/exercise reports** *etc*. demonstrating the effectiveness of the organization's preparations, including but extending far beyond information/IT and indeed information risk and security activities. [ISO 22301 and 22313 are *much* better guides than ISO27k in this area so you may prefer to cite in your SOA and adopt their recommendations]	
A18.1.1 Identifying compliance obligations **A18.1.2 IPR** **A18.1.3 Business records** **A18.1.4 Privacy** **A18.1.5 Crypto laws and regulations**	☐ Specified ☐ In draft ☐ Done	These onerous controls require the organization to identify and maintain concerning *all* **external compliance** requirements/obligations/expectations on the organization relating to [information, risk, IT, IP and] information security and privacy and cryptography, plus IPR (*e.g.* software licenses, patents, trademarks and copyright), plus business records (*e.g.* company finances and shareholdings), implying the need for a managed compliance inventory, database *etc.* with proactive involvement from legal, regulatory, compliance, procurement, IT and security professionals plus others … plus the usual raft of strategies, policies, procedures (*e.g.* periodic updates to the requirements, compliance enforcement and compliance reinforcement/penalties), guidelines and records. Whereas the	

Requirement	Status	Interpretation	Notes
		standard mostly concerns the organization's compliance with external demands or obligations from applicable laws, regulations and contracts, score bonus points for documentary evidence relating to compliance with internal/corporate requirements, including 3rd-party compliance with the organization's contracts, agreements, licenses *etc.* (in addition to compliance with corporate policies, standards *etc.* in the following controls). There should be records concerning the organization's compliance with specific legal, regulatory and contractual requirements such as software licenses, records management policies (retention, destruction *etc.*), policy for protection of personal data, and records of where personal data are held (see also A.8.1).	
A18.2.1 Information security reviews **A18.2.2 Security policy/standards compliance**	☐ Specified ☐ In draft ☐ Done	These controls concern the organization's compliance with **corporate/internal IT and information risk and security obligations**, as demonstrated through policies, procedures and records of reviews, audits, checks, tests, exercises, incidents *etc*.	
A18.2.3 Technical compliance	☐ Specified ☐ In draft ☐ Done	Automated **network vulnerability scanning**, version checks and **penetration testing** may provide regular flows of information, along with **reviews** and/or **audits**.	
*** End of checklist ***			