White paper: Twelve-step transition process from ISO 27001:2005 to 2013 revision

27001 Academy
ISO 27001 and ISO 22301 Online Consultation Center

WHITE PAPER

August 01, 2014

1. Purpose

This white paper is intended for companies that have implemented the ISO 27001 2005 revision, and are planning to transition to the 2013 revision. The paper describes the suggested steps in the process.

2. Other useful resources

For more information about the ISO 27001 2013 revision, see these articles:

- Infographic: New ISO 27001 2013 revision – What has changed?
- A first look at the new ISO 27001:2013
- Main changes in the new ISO 27002 2013
- List of mandatory documents required by ISO 27001 (2013 revision)

3. Timing of the transition

Companies already certified against the ISO/IEC 27001 2005 revision will have a transition period of 2 years to "upgrade" their Information Security Management System (ISMS) to the new 2013 revision.

Since the 2013 revision was published on September 25, 2013, this means that companies will be able to upgrade until September 25, 2015. If your existing ISO 27001 certificate expires after September 25, 2015, then the certification bodies will check if you are compliant with the new revision during the regular surveillance visits; if your certificate expires before September 25, 2015, then you must upgrade by your next re-certification, at the latest.

4. Twelve-step transition process

The easiest way to make the upgrade to the 2013 revision is by following these steps:

1) List all interested parties

You should identify all your interested parties (i.e. stakeholders) – those are persons and companies that can influence your information security or that can be influenced by it (clause 4.2). For example, those are your clients, partners, suppliers, and shareholders, but also could be employees' families, government agencies, local community, media, etc.

Then you have to list all their requirements – contracts, laws, regulations, arrangements, expectations, etc. This will also satisfy the control A.18.1.1.

Once you have this list, it is one of the main inputs for your ISMS – you have to "configure" your ISMS to meet all these requirements.

Read more here: How to identify interested parties according to ISO 27001 and ISO 22301.

2) Define interfaces in the ISMS scope

According to the 2013 revision, as part of your scope definition you need to identify the interfaces between the activities made by your organization and the activities that are performed by third parties (clause 4.3).

For your offices, these interfaces can be, for example, walls and doors; for your IT systems, these can be routers, firewalls and other devices that are the last element you control on your network.

Read more here: Problems with defining the scope in ISO 27001.

3) Align ISMS objectives with company strategy

The 2013 revision requires you to determine the information security objectives compatible with the strategic direction of the company (clause 5.1 a).

You can find out about your company strategy/strategic direction by speaking to a member of top management – probably to the one who has been the sponsor of your ISO 27001 implementation project. Then you need to figure out how your ISMS can help your company achieve strategic objectives, i.e. which benefits it can bring to your business. For example, if you are a cloud provider and part of your company strategy is to provide more reliable service than the competitors', then your ISO 27001 can help achieve that strategic objective because information security not only helps to increase the availability of your systems, but also protects the integrity of the data.

Read more here: Four key benefits of ISO 27001 implementation.

4) Change the top-level Information security policy

This top-level policy doesn't have to be called the ISMS policy anymore, so you can change its title. Further, it doesn't have to include requirements like alignment with strategic risk management, nor the criteria for evaluation of risk, so you can delete those from your policy (clause 5.2).

Although not strictly required, you can include various information security responsibilities in your policy – e.g. who is responsible for the ISMS on the operational level, who is responsible for it on the board level, who will do the measurement and reporting, who will evaluate results, etc.

5) Make changes to your risk assessment process

There are a couple of changes in the 2013 revision: first, you need to identify risk owners for each of your risks (clause 6.1.2 c 2) – you can decide that your risk owners are the same as asset owners, or you can determine that risk owners are persons who have enough authority to manage the risk – e.g. heads of departments.

Second, you don't need to use the methodology based on identifying the assets, threats and vulnerabilities anymore (clause 6.1.2 c 1), so if you wish you can identify your risks in some other (simpler) way – for example, instead of determining separately your laptop as an asset, virus as a threat, and lack of anti-virus software as a vulnerability, you could simply identify this risk as "A laptop could be attacked by a virus." Of course, if you wish, you can keep your asset-threat-vulnerability methodology as it is.

Lastly, you need to identify all the outsourced processes and decide on how to control them (clause 8.1) – although not strictly required in the standard, this is best done during the risk assessment process. To do this, the best way is to include the service of your suppliers and partners as an asset during the risk assessment and identify all the associated risks.

Read more here: What has changed in risk assessment in ISO 27001:2013.

6) Identify status of controls in Statement of Applicability

This is a small change in the 2013 revision, but significant from an implementation point of view – in the SoA you must indicate for each control whether it has been implemented or not (clause 6.1.3 d). You can simply insert a new column where you would indicate status, e.g. "Implemented," "Planned," or "Partially implemented."

(Of course, you will need to change the structure of the controls in SoA, as specified in step 11.)

Read more here: The importance of Statement of Applicability for ISO 27001.

7) Obtain approval from risk owners

According to the new revision, you must ask the risk owners to approve your Risk treatment plan and accept your residual information security risks (clause 6.1.3 f). This is usually done by asking them to approve those two documents; however, if there are too many risk owners the best course is to delegate this responsibility to your top management who will make this approval.

Read more here: Risk owners vs. asset owners in ISO 27001:2013.

8) Plan the communication in a systematic way

You should determine who will communicate to whom, what will be communicated, and when (clause 7.4). This includes both internal and external parties.

Since you have to cover all elements of your ISMS with communication – e.g. risk assessment, risk treatment, controls, measurement, corrective actions, internal audit, etc., the best way to plan such communication is by defining it in each document separately.

For example, in your Risk assessment and treatment methodology you should define who will be informed about the risk assessment results and who should be consulted when the treatment options are determined.

9) Decide what to do with your management procedures

The requirements for preventive actions do not exist anymore (preventive actions basically became a part of the risk assessment process), so you can decide whether to delete that procedure or not.

There are no more requirements to keep the remaining management procedures (Document control, Internal audit, and Corrective action) documented, so you if you wish you can delete those procedures as well, but you must maintain those 3 processes even though they are not documented (clauses 7.5, 9.2 and 10.1).

Generally, smaller companies wishing to decrease the number of documents will be able to work without these documented procedures, whereas for mid-size and larger companies it is probably a better idea to keep those documents.

Read more here: Mandatory documented procedures required by ISO 27001.

10) Write new policies and procedures

If you haven't already written the following documents, you will have to do it now because if you selected related controls as applicable, writing a document became mandatory:

- Secure system engineering principles (control A.14.2.5) – describe how to incorporate security techniques in all architecture layers – business, data, applications and technology.
- Supplier security policy (control A.15.1.1) – describe how the security clauses are inserted in contracts, how the suppliers are monitored, if they observe their security responsibilities, how the changes are made, etc.
- Incident management procedure (control A.16.1.5) – describe how to respond to different types of incidents, who is responsible for what, who must be informed, etc.
- Business continuity procedures (control A.17.1.2) – describe how both the business side of your organization and your IT infrastructure will be recovered in case of a disruption.

Read also: Seven steps for implementing policies and procedures.

11) Reorganize your controls

Annex A got mixed up quite a bit – there are 14 sections now instead of 11, and 114 controls instead of 133. However, most of the old controls remained, while only a handful of new ones appeared: A.6.1.5 Information security in project management, A.14.2.1 Secure development policy, A.14.2.5 Secure system engineering principles, A.14.2.6 Secure development environment, A.14.2.8 System security testing, A.16.1.4 Assessment of and decision on information security events, and A.17.2.1 Availability of information processing facilities.

The only document that will need to be greatly reorganized is the Statement of Applicability; however, it is likely that all the other existing documents will have to be changed slightly. If you have references to controls or clause numbers in your existing documents you have to update those, and also check out if the rules set in your documents are still compatible with the new revision – very likely they are.

Read more here: Main changes in new ISO 27002 2013.

12) Measurement and reporting

Requirements became much stricter in the 2013 revision:

- The objectives should be set in a measurable way (if possible) in order to enable easier measurement (clause 6.2 b) – an example of a measurable information security objective is, e.g., "We want to decrease the number of security incidents by 25% in the following year."

- All activities to address risks and opportunities must be evaluated (6.1.1 e 2) and 6.2j) – this is best achieved through (1) the Risk treatment plan, since it documents how to implement controls that treat risks – you should insert a column in this plan which defines how will the implementation of controls be evaluated; (2) through the Statement of Applicability, by stating the objective next to each control and then measuring if that control has achieved its objective; and (3) in each ISMS policy and procedure you should write by which criteria each document will be evaluated.
- It must be determined what will be monitored and measured, when it will be done, who will do the measuring and who will evaluate the results (9.1); further, the responsibilities for the reporting of the ISMS performance must be clearly assigned (5.3 b) – this is best achieved by describing those responsibilities in a separate document, or perhaps including them in the Information security policy. If you already have a Balanced Scorecard or similar system, you can use it for this purpose of monitoring and measurement.

Read more here: ISO 27001 control objectives – Why are they important?

Sample documentation templates

Here you can download a free preview of the ISO 27001 & ISO 22301 Documentation Toolkit – in this free preview you will be able to see examples of the policies and procedures required by the ISO 27001 2013 revision.

27001 Academy

ISO 27001 and ISO 22301 Online Consultation Center

EPPS Services Ltd.
for electronic business and business consulting
UI. Vladimira Nazora 59, 10000 Zagreb
Croatia, European Union

Email: support@iso27001standard.com
Phone: +385 1 48 34 120
Phone (for U.S. customers): +1(646) 797 2744
Fax: +385 1 556 0711