# ISO 27001 risk assessment: How to match assets, threats and vulnerabilities

The 2013 revision of [ISO 27001](https://advisera.com/27001academy/what-is-iso-27001/?icn=free-what-is-iso-27001&ici=top-iso-27001-txt) allows you to identify risks using any methodology you like; however, the old methodology (defined by the old 2005 revision of ISO 27001), which requires identification of assets, threats and vulnerabilities, is still dominating. (See also: [What has changed in risk assessment in ISO 27001:2013](https://advisera.com/27001academy/knowledgebase/what-has-changed-in-risk-assessment-in-iso-270012013/?icn=free-knowledgebase-27001&ici=top-what-has-changed-in-risk-assessment-in-iso-27001-2013-txt).)

So, how do you combine assets, threats and vulnerabilities in order to identify risks?

How to document the risk identification

Risk identification is the first half of the risk assessment process, after which comes the evaluation part (assessing the impacts and likelihood) – see the details here: [How to write ISO 27001 risk assessment methodology](https://advisera.com/27001academy/knowledgebase/write-iso-27001-risk-assessment-methodology/?icn=free-knowledgebase-27001&ici=top-how-to-write-iso-27001-risk-assessment-methodology-txt).

To make your risk assessment easier, you can use a sheet with assets, threats and vulnerabilities in columns; you should also include some other information like risk ID, risk owners, impact and likelihood, etc.

I found it the easiest to start listing items column by column, not row by row – this means you should list all of your assets first, and only then start finding a couple of threats for each asset, and finally find a couple of vulnerabilities for each threat.

To learn which types of assets you should take into account, read this article: [How to handle Asset register (Asset inventory) according to ISO 27001](https://advisera.com/27001academy/knowledgebase/how-to-handle-asset-register-asset-inventory-according-to-iso-27001/?icn=free-knowledgebase-27001&ici=top-how-to-handle-asset-register-asset-inventory-according-to-iso-27001-txt), and click here to see a catalog of [threats and vulnerabilities](https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/?icn=free-knowledgebase-27001&ici=top-threats-and-vulnerabilities-txt) appropriate for smaller and mid-sized companies.

Relationship between assets, threats and vulnerabilities

So, let’s see what this matching of the three components could look like – for example:

* Asset: paper document:
  + *threat*: fire; *vulnerability*: document is not stored in a fire-proof cabinet (risk related to the loss of availability of the information)
  + *threat*: fire; *vulnerability*: there is no backup of the document (potential loss of availability)
  + *threat*: unauthorized access; *vulnerability*: document is not locked in a cabinet (potential loss of confidentiality)
* Asset: digital document:
  + *threat*: disk failure; *vulnerability*: there is no backup of the document (potential loss of availability)
  + *threat*: virus; *vulnerability*: anti-virus program is not properly updated (potential loss of confidentiality, integrity and availability)
  + *threat*: unauthorized access; *vulnerability*: access control scheme is not properly defined (potential loss of confidentiality, integrity and availability)
  + *threat*: unauthorized access; *vulnerability*: the access was given to too many people (potential loss of confidentiality, integrity and availability)
* Asset: system administrator:
  + *threat*: unavailability of this person; *vulnerability*: there is no replacement for this position (potential loss of availability)
  + *threat*: frequent errors; *vulnerability*: lack of training (potential loss of integrity and availability)
  + etc.

This might seem complicated at first glance, but once you start doing this you’ll see it goes rather quickly. Some people prefer using tools for this kind of work, and I agree this could be a good move for larger companies, but for smaller ones using a tool would only take too much time: [When to use tools for ISO 27001/ISO 22301 and when to avoid them](https://advisera.com/27001academy/blog/2014/10/20/when-to-use-tools-for-iso-27001-iso-22301-and-when-to-avoid-them/?icn=free-blog-27001&ici=bottom-when-to-use-tools-for-iso-27001-iso-22301-and-when-to-avoid-them-txt).

How much is enough?

Very often people ask me – how many risks should they identify? If they start being really thorough, for each asset they could find 10 threats, and for each threat at least 5 vulnerabilities – this is quite realistic, isn’t it?

Now if you are a small company with 50 assets, this would mean you would end up with 2,500 risks, which would probably be overkill for this size of a company. This is why you should focus only on the most important threats and vulnerabilities, while including all the assets; that would mean that per each asset you should identify on average 5 threats, and for each threat on average 2 vulnerabilities. This way you would end up with 500 risks for a smaller company with 50 assets, which is quite manageable.

Why is this methodology still good?

I personally like this assets-threats-vulnerabilities methodology quite a bit – not that I’m nostalgic for the 2005 revision of ISO 27001, but I think this methodology gives a good balance between doing the risk assessment quickly, and at the same time doing it both systematically and detailed enough so that one can pinpoint where the potential security problem is.

And this is what risk assessment is really about: find out about a potential problem before it actually happens. In other words, ISO 27001 tells you: *better safe than sorry*.