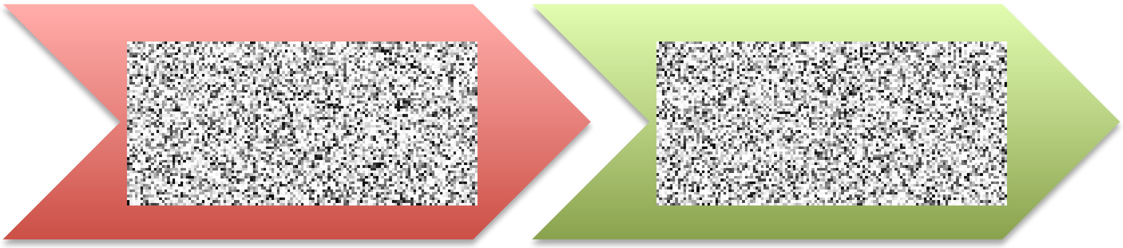


How the ISO 27001 revision affects your risk management process

By Jakob Holm Hansen

Head of Professional Services and Product Management

at Neupart

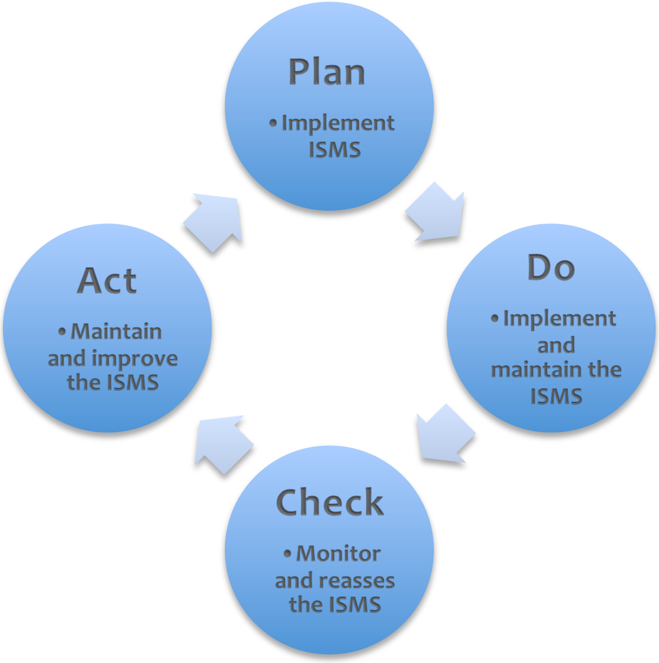
What is different in the new ISO 27001?

ISO 27001:2013 sets the stage for structural changes in the standards individual sections and risk management gets an even more prominent role.

Plan-Do-Check-Act is not explicitly mentioned in ISO 27001:2013, but that doesn't mean it is no longer relevant. The standard mentions "continuous improvement" instead, meaning PDCA is still relevant in the standard although less explicit than in ISO 27001:2005.

It is now called "continuous improvement," and is very much at the core of ISO 27001. The only difference is that companies are now free to choose the way they guarantee continual improvement, be it by PDCA or other types of processes.

It is expected that there will either be a grace period where certified companies can adapt their ISMS and make sure that they meet the requirements in ISO 27001:2013, or a "grandfathering" rule where companies are required to switch as their certificates expires.


Plan
• Implement ISMS
Do
• Implement and maintain the ISMS
Check
• Monitor and reasses the ISMS
Act
• Maintain and improve the ISMS

The rumours of Plan-Do-Check-Act's demise has been greatly exaggerated

The most important changes in ISO 27001:2013 are:

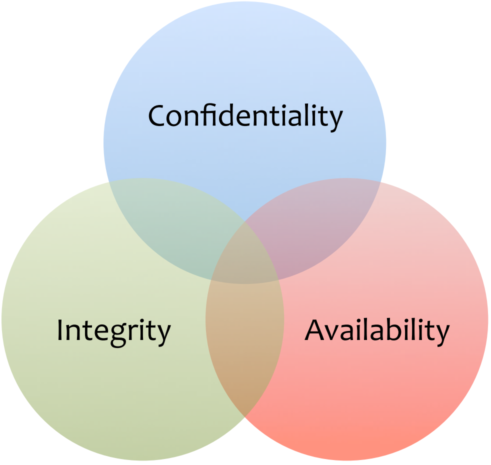
- **New structure**
  With the 2013 edition of ISO 27001, the most obvious change is in the structure. ISO 27001 is now aligned with Annex SL of the ISO directives; meaning that it's structure is comparable to that of ISO 9001.
  In my opinion, it's also a better and clearer structure.

- **Increased flexibility in your choice of risk method**
  In the old ISO 27001 it is a requirement that an "asset owner" is identified and that a threat based vulnerability assessment is implemented.

In the new version "asset owner" is renamed "risk owner," and you are only required to identify risks in relation to confidentiality, integrity and availability.

This is likely an attempt to adapt the risk process to the risk management standard ISO 31000.

The ISO 27005 standard will most likely still be the standard used as starting point for the risk process as it deals specifically with IT risks. ISO 31000 instead provides a framework for analysis of risk types in businesses.



- **Sharpened demands to the Information Security Management System context**
  In the old ISO 27001 the section on establishing the ISMS and the scope is brief and unclear.

  In the new version, the requirements for organisations ISMS context have been highlighted with the requirement that all relevant external shareholder demands must be described as part of the ISMS.

- **Incidents and incident handling are now seen in a broader perspective**
  A new section called "non-conformity" has been added to the standard. Non-conformity covers not only incidents and incident handling, but also all other kinds of non-conformity.

  Non-conformities are, basically, whatever makes you deviate from the ISMS and the controls established in the ISMS. Besides regular security incidents, this could also be findings of deviations from internal audits, as well as gaps in the specified security levels.

- **The demands for monitoring and measuring get their own section**
  In the new ISO 27001, the requirements for surveillance and measurement of efficiency have been given their own section.

  There is an increased focus on ensuring that companies identify, describe and can document the efficiency of the implemented IT controls. For this purpose organisations must draw up Key Performance Indicators for the evaluation of all implemented security measures and be able to document the KPI's output.

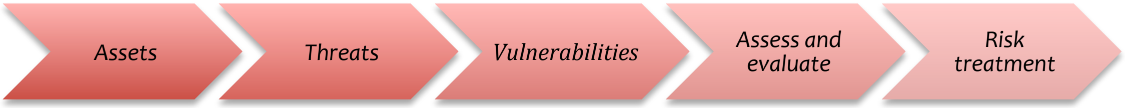
As opposed to the old one, the new ISO 27001 is now focused on function rather than form.

Ok, so how does that affect my risk management process?

If you don’t have a risk management process, you need to get cracking. Because a sound risk management process is more relevant than ever in ISO 27001:2013.

The good news is that if you have a risk management process compliant with the 2005 edition of ISO 27001, your risk management process will most likely still be valid.

This is because the new standard is less specific on the risk management requirements.



Assets → *Threats* → *Vulnerabilities* → *Assess and evaluate* → *Risk treatment*

In the past you needed a risk assessment process that could:

- Identify assets
- Identify threats to assets
- Identify vulnerabilities that might be exploited by the threats
- Analyse and evaluate risks

And a risk treatment process that contained the following specific treatment options:

- Reducing the risk
- Accepting the risk
- Avoiding the risk
- Sharing the risk

This incidentally matches the way ISO 27005 does risk management.

While this way of doing risk management is still best practice – and a very sustainable process – it is no longer a requirement. This means that you can integrate other risk standards and practices into your ISO 27001 programme and still be compliant.

This can be an advantage if you are working in an organisation with an overall Enterprise Risk Management (ERM) programme that you need to integrate into.

> *“Organisations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk”*
>
> *-ISO 31000*

Refreshingly, ISO 27001:2013 also includes "upside risk," instead of only focusing on the normal "downside risk." As a part of your risk management process, you are now also required to identify opportunities, and make sure these are realized.

This could be areas in your ISMS where you have identified an opportunity for your business, by enabling them to do things they weren't able to do before, or deliver new and improved solutions.

Opportunities
Realized business advantage

Risk ownership

Risk ownership is a new concept in ISO 27001. It seems like an offshoot from the "asset owner" in the old ISO 27001.

Risk owners has been introduced for two reasons:

- Firstly, to make ISO 27001 more flexible

By focusing on "risk owners" instead of "asset owners," we are no longer bound by the ISO 27005 requirements of asset ownership, and are free to implement any risk management process that fits our organisation.

- Secondly, to better align with existing ERM processes

Most ERM processes aren't detailed enough to focus on specific assets, but rather look at risk assessing processes or scenarios. If we wish to align to that in our information risk management, then that is possible.

If you wish to continue with ISO 27005 and best practice for IT risk management, the new risk ownership concept won't block that. Effectively, an asset owner in this scenario will be a risk owner on any identified risks on his assets.

A risk owner approves risk treatment plans and accepts residual risks

Risk treatment

Risk treatment is an integral part of risk management and the ISO 27001 standard. Basically, risk treatment is the practice of handling and treating identified and evaluated risks.

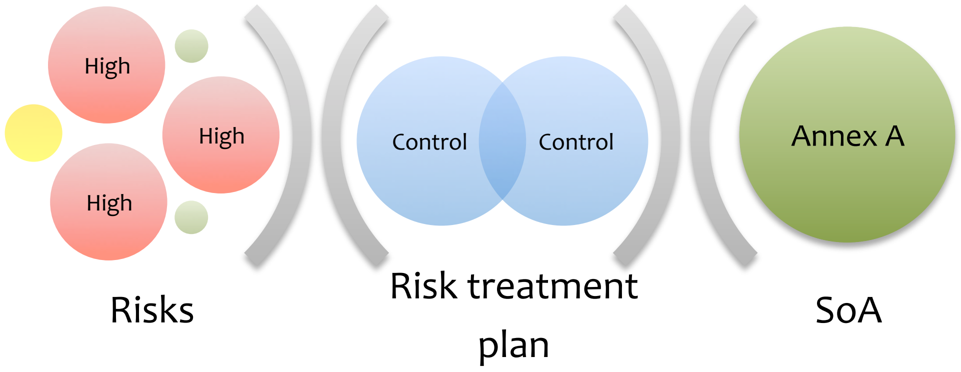
Risk treatment is the last phase of your risk management process. After you have evaluated, assessed and analysed your risks

Like mentioned above, risk treatment is traditionally done by reducing, accepting, avoiding or sharing the risk.

The primary purpose of risk treatment is to integrate with and define the Statement of Applicability in your organisations ISMS.

The Statement of Applicability defines the scope of controls, in Annex A, which the organisation wants to implement. This is why risk management is essential in ISO 27001, it is the instrument we use to define our SoA and thereby our controls.

In ISO 27001:2013, a risk treatment plan is the tool used to create a SoA.



Conclusion

While there are many similarities between ISO 27001:2005 and ISO 27001:2013, there are still some differences.

In practice, you can keep your current risk process, and stay compliant with some minor additions or clarifications:

- Define risk ownership in the context of your organisation and process
- Demonstrate a clear link between risk treatment and your Statement of Applicability

Even though you can continue with your existing risk process, do try to optimize now that you have the increased flexibility.

So, when changing to ISO 27001:2013, our recommendation would be to evaluate your risk process. You could have several reasons for this:

- Maybe you want to integrate better into your company ERM
- Your industry uses a different risk process (OCTAVE, NIST, ISO 31000, etc.)
- You want to take better advantage of risk opportunities

The ISO 27001 standard is currently being revised and is expected to be final in October 2013. This document is based upon the "final draft," but it's highly unlikely that any major changes are going to occur at this stage. So this document won't be out-dated once the final release lands.

SecureAware®

What is SecureAware IT GRC?

Spend less time on security management and get a more precise overview of your security. If you have to comply with standards or best practice for information security, SecureAware gives you improved efficiency and the option to easily assess how much security your organisation needs.

With SecureAware you no longer need complex spread sheets for risk assessments, and you can avoid using lengthy security manuals in countless versions. Further, SecureAware gives you several shortcuts to ISO 27001, PCI DSS-compliance and others. You will also get a complete overview of your recurring security tasks. That way you can spend less time on security management, or you can choose to spend your consultancy budget on other projects.

SecureAware can be used as a full IT GRC solution or as individual modules.

Get more information and a free trial here: www.neupart.com/products

Using SecureAware you will get:

- **ISO 27001 Information Security Management System (ISMS)**
- **Plan-Do-Check-Act process and Statement of Applicability**
- **IT risk management in compliance with ISO 27005 and NIST SP800-37**
- **PCI DSS compliance**
- **Policy and security awareness management**
- **Cloud vendor analysis based on Cloud Security Alliance GRC Stack**
- **Compliance analysis**
- **Control of the security functions**
- **Business Continuity Planning in accordance with BS 25999**
- **Timesaving templates for security policies, business continuity plans and threat catalogue**
- **APIs for data exchange**
- **Smart upgrade ensures easy access to new features and content updates**
- **Runs on several SQL databases**
- **MS Active Directory support with users and groups**
- **Available as a software solution or as a service**

Neupart A/S
Hollandsvej 12
DK-2800 Lyngby
T: +45 7025 8030
www.neupart.com