Vigilant software

5 critical steps to successful ISO 27001 risk assessments

October 2018

www.vigilantsoftware.co.uk | support@vigilant.co.uk | +44 (0) 333 700 1 700

Introduction

Information security threats continually evolve, which is why so many best-practice frameworks, standards and laws mandate an adaptive response based on regular risk assessments: such an approach ensures that the measures your organisation implements are effective and proportionate.

An information security risk assessment will give you an accurate snapshot of the security risks that might compromise the confidentiality, integrity and availability of your organisation's information assets, and can be used to inform the selection and application of appropriate security controls based on business needs and a cost-benefit analysis.

ISO/IEC 27001:2013 (ISO 27001, the Standard) sets out the specification for a best-practice information security management system (ISMS), a risk-based approach to securing corporate information assets that addresses people, processes and technology.

Clause 6.1.2 of ISO 27001 explains that the risk assessment process must:

- Establish and maintain certain information security risk criteria;
- Ensure that repeated risk assessments "produce consistent, valid and comparable results";
- "Identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system";
- Identify the owners of those risks; and
- Analyse and evaluate information security risks according to certain criteria.

Organisations must also "retain documented information about the information security risk assessment process", including two very important documents: the Statement of Applicability and the risk treatment plan. We will discuss them later.

This white paper describes the five steps to completing a successful ISO 27001 risk assessment.

Anyone can follow and apply the best practice set out in this white paper. Most organisations will want to streamline their risk assessment process to improve how quickly best practice becomes embedded. This is most easily done by acquiring and using an ISO 27001 risk assessment software tool, such as vsRisk Cloud.

Five steps to successful risk assessments

1. Establish a risk assessment framework

For risk assessments to be "consistent, valid and comparable" every time they're carried out (as mandated in clause 6.1.2 of ISO 27001), the process must be objective, transparent and auditable. You should therefore establish a formal methodology that will produce consistent results each time, even when followed by different risk assessors. The framework establishes the fundaments of the risk assessment – the key characteristics and parameters that you will take into account throughout the process.

ISO 27001 is supported by a wider family of standards – the ISO/IEC 27000 series – that give more specific guidance on information security. ISO/IEC 27005:2018 (aka ISO 27005) provides guidelines for information security risk management based on the broader risk management process specified in ISO 31000.

Although ISO 27005 is designed to complement ISO 27001, there are many other enterprise risk management frameworks that you can use. Whichever one you choose, it's essential to ensure it fits your purposes.

Baseline security criteria

As part of establishing the context for the ISMS, as required in clauses 4.1 and 4.2 of ISO 27001, your organisation should identify the business, regulatory and contractual requirements it has to meet in respect of information security (for example, the requirements of the General Data Protection Regulation (GDPR), which applies to organisations that process or control the processing of personal information).

We call these requirements the 'baseline security criteria' because they must be accounted for as a minimum. These will be examined as one of the first steps in the risk assessment to ensure that the organisation has correctly identified and implemented the necessary controls to address them. A risk assessment tool will help you identify which controls have been adopted.

Risk scale

The second step is to establish what is called the 'risk scale'. Establishing the risk scale can be one of the most challenging aspects of establishing an ISMS and is one of the areas in which organisations often benefit from external assistance.

Risks are often defined as a combination of likelihood and impact: a risk has to be likely to occur and, if it does, it has to have an impact on the organisation – otherwise, why worry about it?

Generally speaking, you should define impact and likelihood levels that are relevant to your business. Most risk assessments differ in terms of scoring the risk, so it is important is that everyone understands the scoring you use. The basis of measurement can be either qualitative or quantitative.

Likelihood is typically measured as frequency of occurrence (a typical scale might range from 'once per year' to 'every second of every day'). Frequency of occurrence is typically established on the basis of historic evidence and perhaps informed by forecasts of future changes. Typically, the points on the likelihood axis might range from 'highly unlikely' to 'highly likely'.

Impact is more complex, and can involve financial loss, reputational damage, operational disruption and other factors, or some combination of these, all of which have to be reduced to a standard measure.

Considerable effort is usually required to arrive at a basis for determining impact that will be widely understood inside the organisation and, in particular, by those responsible for information security management. Typically, the points on the impact axis might range from 'very low impact' to 'very high impact'.

The risk scale is the number of options your methodology allows for both impact and likelihood. Experienced practitioners know that too much granularity – too many options – makes risk assessment more complex and less consistent.

It can be imagined as a standard graph, where the impact on the organisation is the horizontal axis and the likelihood of an event happening is on the vertical axis. Practice teaches that the optimum risk scale for smaller organisations is a 3 x 3 scale and, for larger organisations, a 5 x 5 scale.

Risk appetite

Your risk scale is used to analyse risks and determine how to respond to identified risks. All organisations are happy to live with – or accept – a certain level of risk. Events that are highly unlikely to happen or that, if they do happen, are highly unlikely to disrupt the organisation might be risks that management is prepared to tolerate – in other words, the sort of risk that management does not consider worth taking action to deal with.

The range of risks that management is prepared to tolerate falls within its 'risk appetite' and can be clearly identified on a risk assessment graph, as shown in the shaded area below.

(very high)	5	Risk Level 5	Risk Level 6	Risk Level 7	Risk Level 8	Risk Level 9
(high)	4	Risk Level 4	Risk Level 5	Risk Level 6	Risk Level 7	Risk Level 8
(medium)	3	**Risk Level 3**	Risk Level 4	Risk Level 5	Risk Level 6	Risk Level 7
(low)	2	**Risk Level 2**	**Risk Level 3**	Risk Level 4	Risk Level 5	Risk Level 6
(very low)	1	**Risk Level 1**	**Risk Level 2**	**Risk Level 3**	Risk Level 4	Risk Level 5
		1 (very low)	(low)	**3** (medium)	**4** (high)	**5** (very high)

Impact

Best-practice risk assessment software should make the process of selecting and working with an appropriate risk scale, and identifying and applying the organisation's risk appetite, relatively straightforward.

Asset-based risk assessment

Good risk assessments should start with a database of critical and valuable assets (for example, records of personal data) and assess events that might affect the security of each asset.

You will therefore need an asset database to support your risk assessment so that you can track risk changes over time in relation to each of your assets.

Good risk assessment tools should therefore have compatible and integral asset databases. Assets can be split into multiple types to ensure that all relevant assets are identified and their owners defined. Asset types to be considered include:

- Information and data (hard copy or digital records);
- Hardware and software (IT assets and business applications);
- Physical locations and storage (sites and office-based stores);
- Systems and services (power, water, gas, lifts, telephony);
- People and organisations (staff, third parties, suppliers, etc.); and
- Intangibles (brand, reputation, share price, etc.).

2. Identify risks

Although identifying risks is relatively straightforward, it is often the most time-consuming part of the whole risk assessment process.

Risks cannot exist without three components:

1. An **asset** that has value and requires protection;
2. A **threat** that can affect it; and
3. A **vulnerability** that allows the threat to affect the asset.

A vulnerability is something that is part of the asset, while a threat is external to the asset (for example, vulnerabilities that exist in unpatched software, which malicious actors seek to exploit through cyber attacks).

Assets can have multiple threats, which can affect them via multiple vulnerabilities. It is therefore important for the lead risk assessor to work with risk and/or asset owners to identify all the events that might compromise the confidentiality, integrity and/or availability of each asset within the scope of the ISMS and, for each event, analyse the risk and determine the likely impact on the organisation.

Good risk assessment software should enable multiple users to work on a shared risk assessment and its supporting database in a way that maintains data integrity and provides a robust audit trail of who has done what.

This is also the time to identify the controls that you already have in place so that you do not waste time unnecessarily duplicating existing measures. Existing controls should also be checked to determine whether they work properly or need to be removed, replaced, modified or supported by other controls.

3. Analyse risks

Risk analysis typically involves understanding how the threat might occur, which usually requires you to identify a vulnerability in your asset and a threat that might exploit that vulnerability.

For each event you identify, you should be able to assess the likelihood of each threat exploiting each individual vulnerability and assign them a score or value.

As established earlier, risks are the product of impact and likelihood.

Impact types could include human, financial, legal, regulatory, reputational and operational.

Likelihood factors could include frequency of occurrence, previous occurrence, current levels of security control, size of attack group and knowledge of vulnerability.

Useful risk assessment software comes with built-in lists of threats and vulnerabilities, usually with appropriate links between them already defined. This removes the need for you to invest time and energy building your own database of threats and vulnerabilities, and should help accelerate and simplify the process of risk analysis. You should also be able to analyse risks on the basis that your baseline security controls are in place and effective.

4. Evaluate risks

Your risk assessment software should automatically collect the results of your risk analysis, calculate where each risk sits on your risk scale and, in particular, identify whether the risk falls within your predetermined level of acceptable risk.

You should very quickly be able to identify your highest risks and, therefore, prioritise which risks to address in what order.

5. Select risk management options

Once you have evaluated each risk and sorted them into order of priority, you should decide how to respond to them. The common responses for each risk are:

- **Modify** – normally by implementing security controls that will reduce likelihood or impact.
- **Retain** – accept that the risk falls within your established risk acceptance criteria, or via extraordinary decisions.
- **Avoid** – end the activity or circumstance causing the risk, for example by not carrying out the activity.
- **Share** – generally by insuring or outsourcing. Although you will typically still suffer the effects, you can share the risk with someone better able to mitigate it.

Your risk assessment methodology should define the criteria that enable these decisions to be made consistently. Your risk assessment software should then, for all the risks that you have decided to treat, provide a range of possible controls that could be applied to reduce the likelihood and/or impact. Ideally, you would want access to the controls listed in Annex A of ISO 27001, as well as those contained in other frameworks, from the PCI DSS to NIST SP 800-53.

Once you've selected controls to reduce identified risks to acceptable levels, you want your risk assessment software to produce the two documents that are required by ISO 27001 – and in a format that will immediately meet those requirements: the Statement of Applicability (SoA) and the risk treatment plan.

Your SoA should:

- Identify the controls you have selected to address the risks you've identified;
- Explain why you have selected them;
- State whether or not they have been implemented; and
- Explain why any ISO 27001 Annex A controls have been omitted.

There will be at least 114 entries in your SoA – one for each Annex A control.

An SoA is a very useful document for everyday operational use – a simple demonstration that controls have been implemented and a useful link to the relevant policies, processes, and other documentation and systems that have been applied to treat each identified risk. Think of it as an index to your ISMS.

How to save time and money on your information security risk assessments
All of this is, obviously, a complex and time-consuming undertaking that, thanks to its reliance on a great deal of human input, is prone to error.

To guarantee that your risk assessment will produce the consistent, valid and comparable results that are essential to the long-term success of your security programme, it is beneficial to use a risk assessment tool.

Introducing vsRisk Cloud

vsRISK CLOUD

vsRisk Cloud is an online tool for conducting ISO 27001-compliant information security risk assessments. It allows users to work from anywhere with an Internet connection and a compatible browser.

With more than ten years of investment, vsRisk Cloud incorporates feedback and experience from hundreds of ISO 27001 risk assessments, and is supported by an ongoing investment and user support programme that regularly adds useful functionality and features to help you continually improve your ISMS.

Features

- Create multiple risk assessments, using either the default settings or customisable options:
  - Customise the ranges of the impact and likelihood scales.
  - Edit the default labels for each point of each scale and add custom labels.
  - Change the values of the default risk acceptance criteria.
- Bulk upload assets to the asset library.
- Use the risk assessment wizard to:
  - Add risks to an assessment.
  - Select controls from eight control sets (the Cyber Essentials scheme, CSA CCM v3, ISO 27001:2005, ISO 27001:2013, ISO 27032:2012, NIST SP 800-53, PCI DSS v3.0, PCI DSS v3.2).
  - Score risks as a combination of likelihood and impact, and see how this affects assets' confidentiality, integrity and availability.

vsRisk Cloud is fully integrable with other products hosted on Vigilant Software's CyberComply platform: Compliance Manager and the Data Flow Mapping Tool.

Stress-free ISO 27001 risk assessments

Find out more about vsRisk Cloud at

www.vigilantsoftware.co.uk/topic/vs-risk

About Vigilant Software

Vigilant Software aims to make implementing cyber security, information security and risk management straightforward and affordable for all. Vigilant Software is part of GRC International Group, globally acknowledged as a leading authority on IT governance and information security.

Drawing on years of experience developing and deploying risk management tools and services, our product range eliminates the complexity of a cyber security implementation project.

For more information about any of our products, please call +44 (0)333 700 1700, email support@vigilantsoftware.co.uk or visit www.vigilantsoftware.co.uk.

Vigilant software