RISK ASSESSMENT SOFTWARE

There are software tools that have been designed to assist in ISO 27001 risk assessment and, although their use is not mandatory in the standard, it is practically impossible to carry out and maintain a useful risk assessment for an organization that has more than about four workstations without using such a tool. It is essential that the risk assessment be completed methodically, systematically and comprehensively. An appropriate software tool, designed with ISO27001 in mind and kept up-to-date in terms of changing information security issues, can be effective in this process.

This is because the risk assessment is a complex and data-rich process. For an organization of any size, the only practical way to carry it out is to create a database that contains details of all the assets within the scope of the ISMS, and then to link, to each asset, the details of its (multiple) threats and (multiple) vulnerabilities, and their likelihood and resulting impacts, together with details of the asset ownership and its confidentiality classification.

The risk assessment process is made enormously simpler if one can also use ready-made databases of threats and vulnerabilities. The database should also contain details of the control decisions made as a result of the risk assessment so that, at a glance, it is easy to see what controls are in place for each asset within the ISMS.

This database must be updated in the light of new risk assessments, which should take place whenever there are changes to the assets or to any aspect of the risk environment. The number of software tools available for this purpose is increasing. To one extent or another they automate the risk assessment process and generate the Statement of Applicability. In theory, such a tool ought to encourage the user to perform a thorough and comprehensive security audit on the organization’s information systems, and ought not to produce too much paperwork as a result. Tool availability is likely to change as the standard is more widely taken up and any organization interested in pursuing this route should therefore do up-to-date research on what is available before making a shortlist.

The organization may need to compare tools before making a selection and should concentrate, in the comparison process, on the extent to which the tool really does easily and effectively automate the risk assessment and statement of applicability development process, the amount of additional paperwork it generates, the flexibility it offers for dealing with changing circumstances and frequent, smaller scale, risk assessments, and the meaningfulness of the results it generates.

Tracking changes to the risk assessment process over time is also of importance, and often the ‘future-proofing’ aspect of requirements of the tool are overlooked during the initial purchase because of the focus on achieving certification, or at least the implementation of an ISO27001-compliant ISMS. Of course, normal due diligence should also be done into the status of the supplier and manufacturer of the product to ensure that it is properly supported and likely to continue to be.

---

Risk assessments can be done without using such tools, although it can be difficult to demonstrate that the risk assessment produces comparable and reproducible results without using such a tool. A proper risk assessment in any business will be very time consuming, whether or not a software tool is used. ‘Time consuming’ means one or more months of dedicated work and, for larger organizations, even longer. The use of a software tool will depend on the culture of the organization and the preferences of the information security adviser and manager.

Practically speaking, once the organization has decided to purchase such a tool, it becomes dependent on that tool and on the staff members who are trained to use it; in considering the appropriate route forward, consideration should be given to the likelihood of being able to recruit staff who have broad risk assessment experience and can adapt to the organization’s environment as against the likelihood of recruiting and retaining staff who have specific experience with one risk assessment tool if that tool requires particular specialist knowledge.

If the organization decides to purchase such a tool, the ISMS project steering group should document the reasons for its choice and selection; whoever is to use it will, of course, have to be fully competent in its use. Evidence of any training and of the level of proficiency achieved should be retained on the personnel file of the person trained in its use.

It is essential to appreciate that risk assessment tools are a specific type of tool, different from other tools such as gap analysis tools, vulnerability assessment tools or penetration testing, each of which is briefly described before we provide guidance on current risk assessment tools.

**Gap analysis tools**

It is important to understand the difference between a gap analysis and an ISO27001-compliant risk assessment. A risk assessment is individual asset-based; a gap analysis assesses the gap between the requirements of a standard or other set of requirements (such as a risk treatment plan or Statement of Applicability) and the controls that are actually in place. Such gap analysis tools almost invariably analyse the gap between the controls in place in an organization and the complete set of those required by the standard. While this exercise can be interesting, it is not deeply useful.

This is because, where ISO27001 is concerned, not all organizations are likely to need to implement all the controls identified in the standard; an analysis of the gap between the requirements of the standard and the current implementation status is not, therefore, particularly useful in the creation of an ISO27001-compliant ISMS. In our analysis, where something identified by the vendor as a ‘risk assessment tool’ is patently only a gap analysis tool, we have clearly identified it as such. There is no point in attempting to use such a tool to carry out the risk assessment component of the ISMS project, because it simply doesn’t meet the requirements of the standard.
**Vulnerability assessment tools**

Vulnerability assessment tools, also called security scanning tools, are also not risk assessment tools as defined by the standard. They do have a role to play in many information security management systems, and that role is determined by the risk treatment plan which arises from the risk assessment. Vulnerability assessment tools assess the security of network or host systems and report system vulnerabilities. These tools are designed to scan networks, servers, firewalls, routers and software applications for vulnerabilities. Generally, the tools can detect known security flaws or bugs in software and hardware, determine if the systems are susceptible to known attacks and exploits, and search for system vulnerabilities such as settings contrary to established security policies.

In evaluating a vulnerability assessment tool, consider how frequently it is updated to include the detection of new weaknesses, security flaws and bugs, and whether or not it refers to common lists of flaws and vulnerabilities such as the SANS Top Twenty, CVE and Bugtraq. Vulnerability assessment tools are not usually run in real-time, but are commonly run on a periodic basis. The tools can generate both technical and management reports, including text, charts and graphs. Vulnerability assessment reports can identify what weaknesses exist and how to fix them.

**Penetration testing**

Penetration testing (or ‘pentesting’) is also not a risk assessment. A penetration analysis is a snapshot of the organization’s security at a specific point in time. It can test the effectiveness of security controls and preparedness measures. Whilst a vulnerability assessment is usually an automated process, using a vulnerability assessment tool, penetration testing usually involves a team of (external) experts who test and identify an information system's vulnerability to attack. They may attempt to bypass security controls by exploiting identified vulnerabilities including, for instance, social engineering, denial of service attacks and other methods. The objective of a penetration analysis is to locate system vulnerabilities so that appropriate corrective steps can be taken.

Pentesting does potentially therefore have a role to play in the ISO27001 risk assessment; it has a more substantial role to play after the assessment, to test the effectiveness of defences that have been installed.

**Risk assessment tools**

Not all of those tools that currently claim to be ISO27001 risk assessment tools are necessarily so, and those that are may in any case not meet your requirements. Different tools target different organizational profiles and are sold under various licence arrangements. Aspects that should be considered in determining the most suitable tool for any one project should include:

- the platform the tool is to run on (laptop, server, ASP server, etc);

---

2 See the discussion, in chapter 9, on technical vulnerability controls.
3 For SANS, CVE and Bugtraq, see the website references in the footnotes on p 109, below.
4 See also the ITGP title *Penetration Testing and ISO27001*, due for publication in early 2008.
• scope of standards compliance (ISO/IEC27001:2005, ISO/IEC 17799:2005, NIST SP800-30, PCI standard, etc);
• scalability (to the needs of the organization and to the number of users);
• flexibility (the ability to divide the process into various sections and run them as discreet assessments in their own right, eg, for business units, or for specific IT systems, or after change to an asset, and then the option to analyse the wider impact on full assessment);
• import (of, for instance, asset lists) and export facility;
• customisable reporting, to suit organizational structures;
• degree of alignment with ISO27001 or with establishing an ISMS (especially any support in producing a Statement of Applicability);
• licence model;
• ease of use (because the more training that is required the higher the total cost of ownership, particularly when you consider back-up expertise);
• price; and
• any requirements for integrating the risk assessment results with another risk management regime.

We have identified the following software tools, each of which claims (to one extent or another) to be an information security risk assessment tool:

• Callio Secura, from Callio Technologies
  www.callio.com
• COBRA
  www.riskworld.net
• CRAMM, in the UK from Insight Consulting
  www.cramm.com
• Ezrisk, from Echelon Consulting
  www.echelonltd.com
• ISRAC, from Infosecure Group
  www.infosecuregroup.com
• Proteus
  www.infogov.com
• PTA (Practical Threat Analysis)
  www.ptatechnologies.com
• RA2 art of risk
  www.aexis.de/RA2Tool.htm
• RiskWatch
  www.riskwatch.com
• RSAM, from Relational Security
  www.relsec.com
• vsRisk™
  www.vigilantsoftware.co.uk
OAT (the OCTAVE Automated Tool) for users of OCTAVE is designed to respond exclusively to the US NIST 800-26\(^5\) standard and has therefore not been considered in this book.

**Risk assessment tool descriptions\(^6\)**

**Callio** has three levels of tool. Callio Secura 17799 is the highest level. It is a team-oriented tool that has been built around ISO17799 and BS7799. It is web-based, which brings with it specific risks that it has not apparently been optimised to control. It contains sample policies, a document manager, an employee awareness centre, a very limited risk assessment tool and a more comprehensive gap analysis tool. It does not perform a risk assessment as required by the standard. More importantly, it appears not to have been updated for ISO27001 and it still contains the control structure of ISO17799:2000, which was withdrawn in 2005. It does not look as though it would be useful for organizations seeking certification to the current standard.

**Cobra** (release 3) is a gap analysis tool (it claims to do an ISO17799 compliance check), not a risk assessment tool, and it appears not to support either risk management or the establishment of the ISMS; at US$895 it’s an expensive gap analysis tool.

**CRAMM** is the oldest risk assessment tool. Version 5 is the current version. It is the preferred tool of the UK government and is recommended by them for use in the public sector. It is widely available through Insight Consulting in the UK and its agents in other countries. It has three modules (CRAMM Express, CRAMM Expert and BS7799 Review). It provides:

- risk assessment and management method;
- business continuity planning support;
- BS7799 compliance gap analysis, security improvement programme, Statement of Applicability and risk treatment reporting; and
- a database of over 3,000 security controls.

The reports CRAMM runs cannot be altered, but there are many pre-defined reports including:

- Countermeasures Status Report and Countermeasures Cost Report; and
- What-If Report.

In support of BS7799 it also offers reports for:

- Information Security Policy;
- Scope of ISMS;
- Gap Analysis; and

\(^5\) NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, was published in 2001 and contains questions designed to enable ‘agency officials to determine the current status of their information security programs’.

\(^6\) The information contained in this section is derived from our own research. Within the limitations of research carried out in a competitive market place, it was valid at the time of the assessment. We emphasise that these are our own assessments; any reader who wishes to review the tools is encouraged to do so.
• Statement of Applicability.

CRAMM appears to meet the key requirements that were set out earlier in this chapter. The customisability of its reports and interfaces is, however, a bit limited. There are two versions available: ‘Express’ (£1,500 plus £250 annual licence) and ‘Expert’ (£2,950 plus £875 annual licence). Insight can deploy its consultancy expertise to help customise the expert version and it recommends that anyone who will be using the tool should undergo their three-day (£1,195) non-residential training programme. It is not, in other words, necessarily as easy to use as they would like it to be. It is, though, the sort of tool that no ISO27001 auditor will object to your having deployed.

**Ezrisk** is a risk assessment tool, but is not ISO27001:2005 compliant and its ISO module appears to be more of a gap analysis tool than a risk assessment one.

**ISRAC** is available in business and enterprise versions and works with ISO17799, not ISO27001. However, it carries out risk assessments at the business process level, not the asset level, and it therefore fails the first requirement of an ISO27001-compliant risk assessment tool. The fact that it treats physical security as an area different from information security (and therefore offers a second module for assessing physical security risks) indicates a fundamental non-conformance to an essential point of the standard, which is that all information, both digital and analogue, has to be protected and that physical controls are as important as logical ones.

**Proteus** appears to be mainly an ISO27001 compliance gap analysis tool. There are various versions available. It does not appear to contain an ISO27001 risk management function. Costs vary from approximately £600 plus licence fee/arrangements upwards.

**PTA** is a risk assessment tool, but was originally designed for use in system specification and does not appear to be ISO27001 compatible in any way. Anyone who wished to use it for an ISO27001 deployment would probably have to invest an uneconomic level of time in customising this product.

**RiskWatch** meets many of the requirements identified earlier in this chapter. It has an effective, comprehensive risk assessment methodology and can assess risk both quantitatively and qualitatively. While it was not built specifically for ISO27001 work, or the establishment and management of an ISMS, it claims that it can apply both ISO17799 and NIST800-26 controls and can be either PC or server-based. While it appears to be a first-class tool, it is also by far the most expensive. A single user licence costs US$14,500. It is probably best suited to larger organizations that require a more sophisticated and granular approach to risk quantification, and to organizations with a US exposure (or that are based in North America) because NIST800-26 compliance is not a requirement outside the US. It is also useful to risk consultants whose offering includes sophisticated, detailed risk assessments at this level.

**RSAM** is a comprehensive, scalable, multi-standard, multi-user, client-server gap analysis tool. It doesn’t follow ISO27001 methodology and it doesn’t produce a Statement of Applicability. It’s not likely to help with an ISMS project.

---

RA2 was developed by two consultants who were deeply involved in both the 2005 revision to ISO17799 and the development of ISO27001. Their risk assessment tool is absolutely in line with the process required by the standard and it can be purchased online. The risk assessment methodology is qualitative and is also in line with the standard. While it is effective for an organization’s initial risk assessment, it is not as obviously capable of comparing assessments and control recommendations made at different times, nor does it easily allow uploading of individual asset details. These two characteristics mean that it is best suited to small to medium organizations, carrying out their first risk assessment as part of their initial ISMS project. It is not self-explanatory to use, but there is no requirement for offsite user training. At £1,100 for a single user licence, it is about half the price of the Expert version of CRAMM. There is no enterprise version.

vsRisk™ This tool has been designed specifically for ISO27001 risk assessments but also supports ISO17799; uniquely, it is also in line with the guidelines of BS7799-3, ISO/IEC TR 13335-3:1998 and both NIST SP 800-26 and SP 800-30. It is also in line with the requirements of the ISF Security Standard 2005 and the Risk Management Standard, developed jointly by the UK’s major risk management organizations. It was developed by a specialist risk management software company to a project brief prepared by the authors of this book, and worldwide marketing rights are held by Vigilant Software™ Ltd. The features of vsRisk™ include:

- Wizard-based approach to simplify and accelerate the process for undertaking risk assessments;
- asset-by-asset identification of threats and vulnerabilities;
- a process to assign all relevant ISO27001 Annex A controls;
- easily imports additional controls to deal with additional risks;
- integrated BS7799-3-compliant threats and vulnerability databases, which are continually updated to ensure that they are the most up-to-date available anywhere, with one year of free updates built into the price);
- customisable management scale and risk acceptance criteria;
- helps define the scope and business requirements, policy and objectives for the ISMS;
- produces an audit-ready Statement of Applicability;
- detailed gap analysis helps drive forward the risk treatment plan;
- integrated audit trail and comparative history;
- helps develop an ISMS asset inventory;
- captures business, legal and contractual requirements against each asset;
- ability to assess confidentiality, integrity and availability against each asset;
- in-built intuitive help feature;
- asset monitor supports import and export of asset information;
- backup and restore capability;

---

8 Information Security Forum, a members-only organization whose Standard of Information Security Good Practice is available from [www.securityforum.org](http://www.securityforum.org).

9 The contributors to the Risk Management Standard were the IRM (Institute of Risk Management), AIRMIC (the Association of Insurance and Risk Managers) and ALARM (the National Forum for Risk Management in the Public Sector).

10 Top Solutions (UK) Ltd ([www.topsolutions.co.uk](http://www.topsolutions.co.uk)), who develop, market and support award-winning risk management software.
• simplifies a business-critical but complex task – meaning external training is not required.

It has been designed with the aim of supporting an ISO27001-compliant risk assessment beyond the first implementation P-D-C-A cycle and has a clear user interface. It does the ISO27001 risk assessment job correctly, easily and efficiently.

**Conclusions**

CRAMM, with its pedigree, is the cautious choice, but is not the easiest or most user-friendly of risk assessment tools. RiskWatch might be the sophisticate’s choice, but the return on investment ratio needs to be carefully calculated, and ISO27001 compliance is not in-built.

RA2 is a tool that complies with ISO27001, and at a reasonable price.

Our view, however, is that, for most organizations, and for consultants providing ISMS services to most organizations, the most appropriate tool – in terms of functionality, ease of use and value for money – is the one that is completely in line with the requirements of ISO27001 as well as all other national and international standards on information security risk assessment, and that is vsRisk™.

**LINKS:**

[www.itgovernance.co.uk/products/789](http://www.itgovernance.co.uk/products/789)

RA2 Art of Risk: [www.itgovernance.co.uk/products/165](http://www.itgovernance.co.uk/products/165)

*™*Risk™: [www.itgovernance.co.uk/products/744](http://www.itgovernance.co.uk/products/744)