ISO/IEC 27005

ISO/IEC 27005:2018 — Information technology — Security techniques — **Information security risk management** (*third edition*)

Introduction

The ISO27k standards are deliberately risk-aligned, meaning that organizations are encouraged to assess risks to their information (called "information security risks" in the ISO27k standards, but in reality they are simply **information risks**) as a prelude to treating them in various ways. Dealing with the most significant **information risks** first makes sense from the practical implementation and management perspectives.

Scope of the standard

The standard 'provides guidelines for information security risk management' and 'supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.'

It cites ISO/IEC 27000 as a normative (essential) standard, and mentions ISO/IEC 27001, ISO/IEC 27002 and ISO 31000 in the content. NIST standards are referenced in the bibliography.

ISO/IEC 27011
ISO/IEC 27013
ISO/IEC 27014
ISO/IEC TR 27016
ISO/IEC 27017
ISO/IEC 27018
ISO/IEC TR 27019
ISO/IEC 27021
ISO/IEC 27022
ISO/IEC TR 27023
ISO/IEC 27030
ISO/IEC 27031
ISO/IEC 27032
ISO/IEC 27033
ISO/IEC 27034
ISO/IEC 27035
ISO/IEC 27036
ISO/IEC 27037
ISO/IEC 27038
ISO/IEC 27039

Content of the standard

At 66 pages, ISO/IEC 27005 is a substantial standard although around two-thirds is comprised of annexes with examples and additional information.

The standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:

- Establish the risk management context (*e.g.* the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization's risk tolerance or appetite);
- Quantitatively or qualitatively assess (*i.e.* identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk';
- Treat (*i.e.* modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those 'levels of risk' to prioritize them;
- Keep stakeholders informed throughout the process; and
- Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.

Extensive appendices provide additional information, primarily examples to demonstrate the recommended approach.

Status of the standard

The first and second editions are ancient history.

The *third* edition of ISO/IEC 27005 was published in **2018**. This is a "minor revision", a temporary stop-gap measure with very limited changes - the main one being that references to ISO/IEC 27001 now cite the 2013 edition).

A project to revise/rewrite the standard made insufficient progress and was cancelled ... and then re-started. Development of the *fourth* edition of '27005 is under way. Hopefully, the *fourth* edition of ISO/IEC 27005 will be published at about the same time as the next release of ISO/IEC 27001, supporting the updated ISMS specification ... but that's not guaranteed. A substantial volume of comments including some fundamental issues with the process of information risk management indicate that this project is, once more, tackling a rocky uphill path, in slippers, in Winter.

ISO/IEC 27040
ISO/IEC 27041
ISO/IEC 27042
ISO/IEC 27043
ISO/IEC 27045
ISO/IEC 27050
ISO/IEC 27070
ISO/IEC 27071
ISO/IEC 27099
ISO/IEC TS 27100
ISO/IEC 27101
ISO/IEC 27102
ISO/IEC TR 27103
ISO/IEC TR 27550
ISO/IEC 27551
ISO/IEC 27553
ISO/IEC 27554
ISO/IEC 27555
ISO/IEC 27556
ISO/IEC TS 27570

The fourth edition is at **W**orking **D**raft stage.

Further reading

Read more about selecting suitable information risk analysis methods and management tools in the ISO27k FAQ.

Personal comments

The introduction to the draft *fourth* edition says it is "based on the asset, threat and vulnerability risk identification method [per ISO/IEC 27001:2005] that is no longer required by ISO/IEC 27001[:2013]", lamely noting that "There are some other methods that can be used." It goes on to state that the standard "does not contain direct guidance on the implementation of the ISMS requirements given in ISO/IEC 27001" [presumably meaning clause 6.1] and the standard "supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach", so make of that ambiguity what you will.

The draft *fourth* edition's working title "Guidance on managing information security risks and opportunities" gives a strong hint that it will directly support section 6.1 of ISO/IEC 27001:2013 ("*Actions to address risks and opportunities*"), mostly concerning the risks in fact: whether 'opportunities' and ISO 31000 get much of a look-in remains to be seen. Regarding ISO/IEC 27001 section 6.1, I believe JTC1 intended that section to have addressed risks to and opportunities for the *management system*, not for *information* or even *information security*, a crucial distinction. If that's true, and if the fourth edition of 27005 explicitly supports 6.1, then logically it ought to concern the management of risks and opportunities to the ISMS, not to information. However, the 6.1 boilerplate wording imposed by JTC1 on all the management systems standards is ambiguous.

Talking of opportunities, rewriting 27005 presents a golden opportunity for SC 27 to reframe it as a standard on **information risk management** where '**information risk**' might be defined along the lines of "**risk pertaining to information**". Among other things, that would remove references to 'information security risk', a curiosity of the current standards. What is that, exactly? It is not explicitly defined as a term. A note to the definition of *risk* in ISO/IEC 27000 refers to it as the "effect of uncertainty on information security objectives". A note to the definition of *objective* says, rather enigmatically, "information security objectives are set by the organization, consistent with the information security policy, to achieve specific results." So, stitching those two together, information security risk is defined as "the effect of uncertainty on information security objectives set by the organization, consistent with the information security policy, to achieve specific results". Frankly I'm none the wiser, if anything more confused by the tortuous and unhelpful explanation.

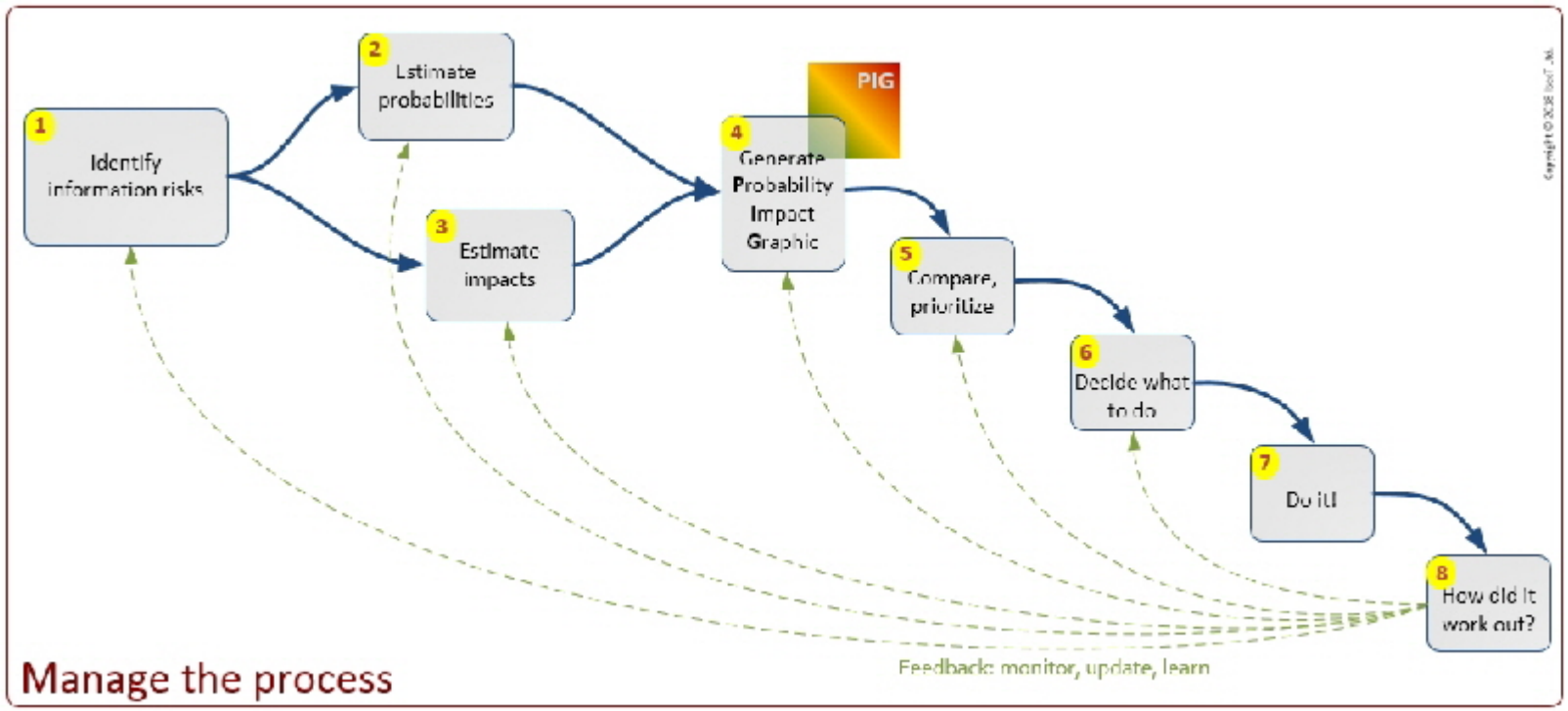
ISO/IEC 27701

ISO 27799

Other ISO27k

A re-framed standard on **information risk management** could underpin *all* of ISO/IEC 27001, not just section 6.1. Given that the entire ISO27k approach is supposedly risk-aligned, identifying, evaluating and treating **information risks** is a fundamental element, hence a standard on **information risk management** is fundamental. There are lots of areas where it could offer useful advice *e.g.*:

- Explain what 'information risk' is, for starters - defining it formally (properly), clearly, helpfully and without the torture and ambiguity of the current gibberish, and then explaining it in more accessible and understandable terms;
- Outline the organizational/business context for information risk management - how it relates to the management of other kinds of risk, and how risk management supports management and governance of the organization;
- Outline the core risk management process roughly along these lines:



- Elaborate on each of those activities in more depth, offering pragmatic advice on suitable methods and approaches (*e.g.* the four ways to treat risk; how to measure, evaluate and compare risks; how to spot and react to changes, and how to predict changes using trends, statistical techniques and situational awareness);

- Describe the process management and governance aspects *e.g.* scoping and setting objectives, planning and resourcing, forming a competent team, documenting the work, reviewing and authorizing things, and handling issues;
- Explain the links to related concepts, citing relevant standards *e.g.:*
  - Sound reasons for consciously and deliberately taking risks - the upside or opportunities arising;
  - Accountability and responsibility, plus the concept of information [risk] ownership;
  - IT or cyber-risks - specifically relating to networks, IT systems, data, applications, coding and technology;
  - Non-IT/cyber information risks *e.g.* those relating to people, intellectual property, tangible assets, compliance and more;
  - Mitigating **information risks** using information security controls, *where appropriate* (noting that security controls are *not* necessarily necessary, despite what infosec pro's commonly think);
  - Business continuity management and cyberinsurance;
  - Cloud, supplier/partner/customer relationship management and the community, social and societal aspects of information risk.

- An appendix, perhaps, with advice on different methods, systems and approaches to **information risk management**, risk assessment, risk analysis, risk treatment *etc.* including those from other fields *e.g*. commercial risks, health and safety risks, environmental risks, technology risks, innovation risks, strategic risks, relationship risks, project risks, financial risks ...

Meanwhile, it has been suggested (by British Standards) that ISO/IEC 27005 should be largely replaced by BS7799-3:2017 ... which has the merit of expediency, and brings ISO27k neatly back to its roots.

< Previous standard ^ Up a level ^ Next standard >