ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection"
Secretariat: **DIN**
Committee manager: **Mahmoud Sobhi Mr**

SC27 Journal Vol 2 Issue 2 (update Dec 2022)

Document type	Related content	Document date	Expected action
General / Other		2023-01-18	**INFO**

ISO/IEC JTC 1/SC 27/AG 7 "Communication and Outreach (AG-CO)"
Convenorship: **BSI**
Convenor: **Humphreys Edward Prof.**

SC27 Journal Vol 2 Issue 2 (update Dec 2022)

Document type	Related content	Document date	Expected action
General / Other		2023-01-17	

SC 27 Journal

Volume 2, Issue 2 (update), 17th Dec 2022

JTC 1/SC 27
Information security, cybersecurity and privacy protection

VOLUME 2, ISSUE 2 (UPDATE)

ISO/IEC 27002:2022

17TH DEC 2022

The views and opinions expressed in the articles in this Journal are those of the author(s) and do not necessarily reflect the views or opinions of ISO, IEC, JTC 1, SC 27 or the editor of this publication.

ISO, IEC, SC 27, the editor and the authors shall not be liable regarding the use, interpretation or implementation of the material contained in any of the articles contained in this publication.

© ISO 2022

CONTENTS

Prologue 7

Words from the SC 27 Chair 8

Once Upon A time 9

ISO/IEC 27002:2022 - Information security controls 13

ISO/IEC 27002 Legacy and future from a Swedish perspective 16

Realising the full benefits of ISO/IEC 27002:2022 21

Inventory of information and other associated assets 29

STORAGE SECURITY and ISO/IEC 27002 35

Introducing the new control on cloud security in ISO/IEC 27002 39

Hall of Fame 51

Author Bios 53

PROLOGUE

Welcome to a update of Issue 2 (Volume 2) of the ISO/IEC JTC 1/ SC 27 Journal. The purpose of Journal is to present articles from SC 27 experts involved in the development of standards covering information security, cybersecurity and privacy protection.

This current issue covers articles celebrating the exciting third edition of ISO/IEC 27002:2022, This new edition is expected to continue the outstanding success of previous versions, providing a much needed set of information security controls for use by all types of organisations, across all business sectors and globally in all countries.

Any questions or feedback relating to the content of this Journal can be directed to editor (sc27.wg1.edwardjh@gmail.com)

Dr Edward Humphreys
SC 27 Journal Editor
Dec 2022

WORDS FROM THE SC 27 CHAIR

Dr Andreas WOLF (SC 27 Chair)

The publication of ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls marks a milestone in the development of the ISO/IEC 27000 family of standards. This third edition further improves the already excellent set of security controls applicable for literally all IT security test and assurance purposes.

ISO/IEC 27002 is marked as high impact standard in the ISO Project Portal. There is a reason for this mark, as this document is one of the key components of the entire 27000 family concept. It is remarkable that the development of this 2022 edition mostly took place during the COVID-19 pandemic. All stages starting with the first Committee Draft took place using virtual collaboration tools. These additional challenges did not prevent the team of Editors Sabrina Feng, Alia Fourati, and Veronica Marinelli from leading their project safely through hundreds of pages of comments provided by the SC 27 National Bodies and their experts. The team finalised the standard in time, also maintaining the expected superior quality.

I would like to thank in particular the 27002 Editors and all experts contributing to the development of the SC 27 flagship standard ISO/IEC 27002:2022.

ONCE UPON A TIME

Dr Edward HUMPHREYS (SC 27/WG 1 Convenor)

It is the March 1988 and I had arrived in San Francisco international airport on my way to an I^4 meeting at Stanford Research Institute (SRI) International, Menlo Park. The meeting discussion I was looking forward to was the debate of baseline controls for information/IT security. The I^4 group[1] were developing a baseline security methodology based on industry best practice. The work involved US companies and various companies from Europe (e.g. from Finland, Germany, Netherlands, UK). The baseline security concept presented management and security administrators with a number of benefits with the satisfaction of knowing that the controls they are using are in general use by other, well-run organisations. From this evolved the development of *common-use criteria,* that is, a control was considered to be a baseline control if it meet the criteria without the need for further assessment before use.

CODES OF PRACTICE

By late 1989 code of practices using the notion of the I^4 baseline controls were being incorporated into operational use by many organisations. One of these organisations in the UK developed an extended code of practice which they shared with a number of other UK organisations. This code of practice added to the *common-use criteria* the notion of risk, thus introducing the idea of baseline methodology and risk-based methodology combined. This eventually became a UK industry code practice, which the UK government supported and promoted. Organizations from

[1] International Information Integrity Institute (I^4)

other countries became interested in using this code, publishing it as a national code and sharing their experiences in its use. The benefits of using this code of practice was soon to be realised by many organisations in a diverse range of industries. Other countries and organisations developed baseline standards, for example, the German Bundesamt für Sicherheit in der Informationstechnik BSI (Baseline Protection Manual), ISACA CoBIT baseline security, NIST control baseline standards, and Australian/New Zealand baseline standards.

BS 7799-1, ISO/IEC 17799 AND ISO/IEC 27002

The UK industry code of practice became the standard BS 7799-1 in 1995 and consequently became a national standard in various countries. After years of business and technology changes and developments a revision of BS 7799-1 was undertaken, involving experts from UK and from Australia, Brazil, Denmark, Germany, Ireland, Japan, Korea, Netherlands, Norway, Sweden and Switzerland. Subsequently ISO/IEC 17799, the international version arrived, based on BS 7799-1. As the WG 1 convenor, I introduced the ISO/IEC 27000 family, and ISO/IEC 17799 was subsequently renumbered as ISO/IEC 27002. After this ISO/IEC revisions in 2013 and 2022 have brought us up to date with today's business needs for information security controls as the times changed.

Another aspect we should not forget is the development of the ISO/IEC 13335 group of standards dealing with Management of IT Security (GMITS) which were developed and matured 1991-2002. In particular the baseline approach to risk features in ISO/IEC 13335-3. The ISO/IEC 13335 family, which also adopted a baseline approach, was phased out around 2002 to be replaced by the ISO/IEC 27000 family. The ISO/IEC 13555 family made a significant impact on security management standards in SC 27

and together with BS 7799-1 (ISO/IEC 27002) transformed our view of the future.

THE TIMES ARE CHANGING AND HAVE CHANGED

The past thirty years have seen many significant changes in business and society, with technology transforming the way we work, live and play. Also, these changes have meant our ways and methods of protecting our information have had to change to keep-up with the rapid advances in new technologies, applications of this technology and our greater access to on-line connectivity. In the 80s the concept of baseline security seemed adequate but the next decade meant we needed to expand this concept to a more pro-active way of addressing risks. Certainly the baseline methodology was a starting point for finding a common language to address information security management. The 90s saw this search for a common language continue boosted by BS 7799-1:1995 and global outreach. Today, the philosophy of baseline security combined with the risk-based methodology continues to be part of our defence against to our information. The past, present and future of ISO/IEC 27002 is founded on the baseline approach combined with the risk-based methodology and the business criteria that has evolved over 35 years of development.

[1] HUMPHREYS, Edward Dr. - Finding a language to address information security management (ISO Bulletin, Dec 2000)

[2] SAARI,Juhani and PARKER, Don - New Baseline methodology in reviewing security - experiences from the USA and Finland (Information Age, volume 11, No.1 Jan 1989)

[3] HUMPHREYS, Edward Dr. - Historical Account of the Development of ISMS Standards (1990-2019) (International ISMS Journal, June 2022)

[4] BSI DISC PD007 Guide to the BSI Code of Practice for information security management (1995)

[5] CoBIT Security Baseline (IT Governance Institute, ISACA, Jan 2007)

[6] IUA (International Underwriters Association), London and UK/DTI - Assess and managing digital risks (2005)

[7] HUMPHREYS, Edward Dr. - ISO/IEC 13335-3 and the Baseline Risk Method of the Development of ISMS Standards (1990-2019) (ISO Bulletin, Mar 2002)

ISO/IEC 27002:2022 - INFORMATION SECURITY CONTROLS

Sabrina FENG, Alia FOURATI, Veronica MARINELLI
(ISO/IEC 27002:2022 editors)

BACKGROUND AND OVERVIEW

ISO/IEC 27002 is one of the most widely used and adopted standards on Information Security controls in the world. It provides a list of general information security controls and guidance to implement these controls. Organizations can use it as standalone guidance or to support the implementation of an Information Security Management System compliant with ISO/IEC 27001.

The standard was first published in 2000 as ISO/IEC 17799, which adopted a British Standard known as BS 7799-1 originally published in 1995. ISO/IEC 17799 was subsequently renamed to ISO/IEC 27002 and revised in 2005, then in 2013, and most recently revised in 2022, which became the 3rd edition.

The standard now has 93 controls compared to the 114 controls in the 2nd edition. The main changes are related to the structure of the document, the addition of attributes and to bring the list of controls up to date, as well as reduce redundancies.

WHAT'S NEW ON THE 3RD EDITION?

NEW STRUCTURE

In the revised version, the controls are organized through 4 themes: 37 organizational, 8 people, 14 physical and 34

technological controls. Each control has now an individual purpose in addition to the control text, guidance and additional information. Some of the guidance has been structured with subheadings to be used as pointers to specific content. Attributes have been added to each control. This simplified structure has allowed controls to be merged, reducing redundancies.

New terms and definitions that are considered necessary to understand the document have been added to Clause 3.

Two new Annexes have been added: Annex A related to the use of attributes and Annex B for the correspondence of controls between this edition and the previous one and vice versa.

ATTRIBUTES

Five attributes are added to each control to allow creating different views or categorizations of controls. Organizations can define their own attributes and associated values to create views that fit their purposes. The added value provided by these new attributes is that they make the standard more flexible so that organizations can create their own views to present, filter or sort the controls for different audiences, perspectives and needs. They could also be used to ease proof of compliance with IS requirements, laws, regulations and frameworks through the use of the controls and guidance included in ISO/IEC 27002.

UPDATED GUIDANCE AND NEW CONTROLS

The guidance in all controls has been updated to the current international best practice according to the state of the art.. 11 new controls have been added and 24 of the current controls have resulted from mergers of previously existing controls for

which guidance has been updated as well as redundancy eliminated.

THE FUTURE OF RELATED SC 27 STANDARDS

The controls in ISO/IEC 27002 are included as Annex A in ISO/IEC 27001. Current version of ISO/IEC 27001, 6.1.3 Risk Treatment Plan, requires organizations to compare the controls implemented by the organization to those listed in Annex A and produce a Statement of Applicability which justifies the inclusion and exclusion of the Annex A controls. ISO/IEC 27001:2013/Amd 1 is now at DIS stage, so an updated version in which Annex A corresponds to the controls in ISO/IEC 27002:2022 will probably be available within the first semester of 2022.

In the ISO/IEC 27000 family of standards, there are several sector-specific standards developed to provide guidance for specific sectors. ISO/IEC 27701:2019, a discipline-specific standard, proposes a Privacy Information Management System based on the extension of ISO/IEC 27001 and ISO/IEC 27002. The revision of some of these has already begun, like ISO/IEC 27011, ISO/IEC 27019, ISO 27799 and others will certainly follow suit soon. The implementation guidance of ISO/IEC 27002 controls is high level and, in some cases, refers to other ISO/IEC standards that provide additional specific control guidance.

ISO/IEC 27002 LEGACY AND FUTURE FROM A SWEDISH PERSPECTIVE

Jan BRANZELL (SC 27/WG 1 and Swedish expert)

Looking at 20 years of experience of ISO/IEC 27002 in three stages:

- *Early days*
- *The 2013 version*
- *2022 and the future*

THE EARLY DAYS AROUND THE NEW MILLENNIUM.

In 1999 I came across the newly published Swedish standard SS-627799. That was a Swedish translated version of BS 7799 "Code of practice for information security management". Little did I know then that I should write an article on my view on how this document has been used during its transformation into ISO/IEC 27002:2022.

In those early days the reason for me and other experts in Sweden to look at this document was that apart from technical standards, this document was the only one that took a broad approach to information security so that both technical and organizational controls can be covered. Obviously, there was a control focus and very much of the guidance text was used and assured. The document did get some criticism from IT security experts that it did not say exactly what should be done. But this was also seen as an advantage because the absence of technical details and the way the controls were described enabled a non-technical expert to get a good understanding. My personal aim was to use a standard that covered these three perspectives:

- Organizational – meaning that controls cover what you need to do as an organization in addition or to support technical security as well as handling personnel.
- Physical security – meaning the traditional technical controls but with a clear purpose of protecting information, digital or on paper.
- ICT security – meaning the technical controls you can apply to your ICT environment also including routines and procedures related to ICT.

It is of course interesting to note that the 2022 version of ISO/IEC 27002 still has the same coverage and that the new structure with "Organizational", People", Physical and Technology" follows the same approach 20 years later. I still remember one of the security officers from a business unit in the organization I was working with at that time stating: "It is fine that you from the corporate side implement encryption solutions over the internet, but we still do not know who is entering our reception". The need for a holistic view was true then and still is.

Then ISMS was added as a Swedish standard as SS 627799-2 in 2003 and then as ISO/IEC 27001 in 2005. More Swedish experts started looking at both standards and they often had a background with other management system standards and in particular ISO 9000. The interest in certification started but was very limited as information security still was linked to IT security. The concept of the standards and the certification was at the time misinterpreted for being mainly about documentation which I believe came from the experience of ISO 9000 work. This was a very unfortunate perception and I believe this slowed the use of ISO/IEC 27001 in Sweden down, and ISO/IEC 27002 was still the dominant standard that organizations used. Swedish experts

including myself, tried to support the use of both standards by the work of ISO/IEC 27003:2010 version that presented implementation guidance on ISMS.

USING THE 2013 REVISION

When the revisions of both ISO/IEC 27001 and 27002 came in 2013 there was a shift and a more complete use of an ISMS started to grow in Sweden. The risk-based approach in ISO/IEC 27001 and understanding of Annex A got better even if many organizations still used Annex A as a check list rather than a reference list. Those organizations that looked more into ISO/IEC 27002 had a real advantage of realizing that the short control statements in ISO/IEC 27001 Annex A was not sufficient to understand what a control really could be in practice. When in 2013 I started working as an editor for the revision of ISO/IEC 27003 the view got much clearer that ISO/IEC 27001 requirements are essential for a robust and systematic approach to information security in the long run, while controls and their implementation as per ISO/IEC 27002 can vary greatly depending on the context of the organization and the risk landscape. I started to describe the different standards as:

- ISO/IEC 27001 – The ingredients for a systemic management approach to information and cyber security.
- ISO/IEC 27003 – The cookbook on how to use those ingredients to suit the organization.
- ISO/IEC 27002 – Also a cookbook but then on how to use and implement the controls in ISO/IEC 27001 Annex A for addressing the risks.

Without the controls implemented the security that the organization needs will not be in place. By combining the

implementation of controls with the requirements in ISO/IEC 27001 the organization can use controls in an effective way over time. The two standards play together for better and effective security which should be any organization's motive to start with. Now also the interest in the ISO 27000 series, as the three plus standards were referred to in Sweden, was more established and their use was recommended for governmental agencies etc. and certification started to be required in certain market sectors.

ISO/IEC 27002 IN 2022 AND THE FUTURE

The holistic approach of ISO/IEC 27002 is even more apparent with the 2022 version with its four main clauses:

- Clause 5 Organizational controls – which can be seen as controls that apply to the organization as such and cannot be directly related to risk in the same way as within the context of the other three clauses
- Clause 6 People controls - which can be applied to risks related to people
- Clause 7 Physical controls - which can be applied to risks related to physical resources
- Clause 8 Technological controls - which can be applied to risks related to ICT resources

This structure should make it easier to see where a control can apply depending on the context of the risk and relate to who/what function in an organization that is responsible for implementing the control.

Today when an organization may face different control sets, the basis in ISO/IEC 27002:2022 control structure should make it easier to link controls from other sources to see if they are

addressed in ISO/IEC 27002 or additional controls may be added. It should now with the new structure be much easier to use ISO/IEC 27002 controls as the basis for information security management and the standard can serve as a common reference list in a dialogue between two parties. Of course, this reference may also support the use of Annex A in ISO/IEC 27001 when this will be updated. Thus, the use of the new version may have a strong impact as a guidance and support for structuring the information security in a more flexible but still structured and transparent way.

Sometime in the future if I may speculate, there might be an additional clause – "Cyber space controls". This if we succeed in in the future having a clear definition of what cyber space is I am sure we can find controls that go beyond the organization and can be applied to the cyber space. The future will hopefully tell and in the meantime, the four existing clauses in 2022 version of ISO/IEC 27002 will take us much further in terms of information security, cyber security and privacy than where we were in 2013.

REALISING THE FULL BENEFITS OF ISO/IEC 27002:2022

Dr David BREWER
(SC 27/WG 1 and United Kingdom expert)

INTRODUCTION

The third edition of ISO/IEC 27002:2022 was published in February this year with a minor correction in March. The new edition presents a wide range of information security controls, grouped as being organizational, people, physical and technological controls. There are 93 controls formed from the 114 controls in the previous edition of the standard together with 11 new controls.

These 93 controls will provide the content for Annex A to the third edition of ISO/IEC 27001, anticipated later this year. This revision will ultimately require organizations to recompare their necessary controls with those in the revised Annex A. In turn, this may require them to implement new controls, should the recomparison discover any inadvertently omitted necessary controls.

The purpose of an information security control, perhaps in combination with other controls, is to modify risk. Controls are referred to as being “necessary” if they assist to modify the risks to which an organization is exposed. Thus, an inadvertently omitted necessary control implies that the organization is exposed to a risk that it has been perhaps ignorant of for some time. It therefore follows that the third edition of ISO/IEC 27001 will directly assist organizations to reduce their exposure to risk, or at least increase their confidence in having done so. This is a

clear benefit of ISO/IEC 27002:2022. Nevertheless, there are other benefits, which we will present in this article. They are:

- using the guidance text in ISO/IEC 27002 significantly increases the effectiveness of the Annex A comparison exercise;
- using custom attributes can find gaps in an organisation's risk treatment plan;
- using control-event scenario mapping to find applicable risks that an organisation has omitted to consider.

USING THE GUIDANCE TEXT OF ISO/IEC 27002:2022 IN THE COMPARISON PROCESS

One way an organization can compare its necessary controls with those in ISO/IEC 27001 Annex A is to convert the control text in into a question. For example, A.8.13:

> "Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup"

becomes

> "Do you backup, maintain and regularly test copies of information, software and systems in accordance with your agreed topic-specific policy on backup".

If the answer to this question is "yes", then the organisation could describe its corresponding necessary control in its Statement of Applicability (SOA) as the statement form of this question, i.e.:

> "We backup, maintain and regularly test copies of information, software and systems in accordance with our agreed topic-specific policy on backup".

Note that the statement form is a statement of fact (present tense) and not a statement of requirement ("shall") or recommendation ("should").

If the answer to this question is "no", then the organization has excluded the A.8.13 control and is therefore obliged to justify that exclusion in its SOA, perhaps individually or collectively with other excluded Annex A controls.

A third possibility is that the organization could give the answer "similar" and then replace this question with one to which it could answer "yes". For example, the statement form of such a replacement question could be:

> "Our data files are automatically backed up as work proceeds and we can recover previous and lost versions. Our data files are stored in the Cloud and on RAID 1 mirrored discs. In addition, we take periodic disc images of our operating systems, operations software, and configuration data, which are verified prior to completion".

This is a variation of the Annex A control and thereby does not exclude A.8.13. (Variations are discussed in ISO/IEC 27007).

Study of the guidance text for 8.13 in ISO/IEC 27002:2022 inspires two additional questions:

A. Do you ensure that inadvertent data loss is detected before backups are taken?

B. Do you restore the appropriate backup(s) to recover all essential information and software following a disaster or media failure?

The answers to these questions can be “yes”, “no” or “similar” as before. However, in this case, the answer “no” does not trigger the need for a justification in the SOA, because the questions do not correspond to an ISO/IEC 27001 Annex A control. Nevertheless, if an organisation does not restore the appropriate backups following a disaster or media failure, the utility of taking the backup in the first place is lost. Moreover, if inadvertent data loss is not detected, restoring the backup will not recover the lost data rendering the backup somewhat useless. These two supplementary questions are therefore important questions to ask. Asking them increases the effectiveness of the ISO/IEC 27001, Clause 6.1.3 c) comparison process.

Study of ISO/IEC 27002:2022 has led the author to identify 161 such questions in total. Since 93 of these correspond to the 93 Annex A controls, 68 correspond to questions arising from the ISO/IEC 27002:2022 guidance text. This is a significant number.

USING CUSTOM ATTRIBUTES TO FIND GAPS IN AN ORGANIZATION’S RISK TREATMENT PLANS

The SC 27?WG 1 Utility of the SOA study reported that some respondents regarded risk treatment plans (RTPs) as specifying the inter-relationship between necessary controls, whereas other respondents regarded them as implementation plans. Taking the former view, a RTP can be laid out in a storyboard format using separate clauses for preventive controls, detective controls and reactive controls in that order.

Since some reactive controls only modify the security of a single consequence, if an RTP addresses several consequences, the clause concerning reactive controls is partitioned into subclauses, one for each such consequence.

Research conducted by the author (based on the original research conducted by Brewer and Nash – "Insights into the ISO/IEC 27001 Annex A, 2010) uses 12 events which collectively address the risks mitigated by the 114 Edition 2 controls.

Using the ISO/IEC 27002:2022 concept of a custom attribute, custom attributes, namely event, consequence (confidentiality, integrity, availability), type (preventive, detective, reactive) are associated with each necessary control depending on its location in the RTPs. For example, RTP-S1 represents events concerning the theft or loss of a mobile device and is associated with the loss of confidentiality and availability. A necessary control placed in the detective clause of RTP-S1, would therefore be associated with the attributes:

- Event: S1
- Type: D
- Consequence: CA

Note that these consequence and type attributes differ from their namesakes in ISO/IEC 27002:2022. The former attributes take their values from the way the control is used in the RTPs. If a control appears in more the one RTP it will potentially take on multiple contrasting values depending on how it is used. The example attributes presented in ISO/IEC 27002:2022 cannot do this, as ISO/IEC 27002:2022 by necessity is ignorant of user defined events.

Having associated the necessary controls with the 12 RTPs in this way, one would hope that each prevent, detect, and react clause would be populated. The reason for this is that if the preventive controls fail, the detective controls should allow the organisation to act promptly to prevent the consequence. If that fails, the reactive controls are intended to reduce the severity of the consequence, so the overall impact on the organizations need not be as bad as otherwise it could. RTPs designed in this way therefore offer resilience to control failures.

Even after populating the RTPs with the 161 necessary controls as derived from the study of ISO/IEC 27002:2022 described above, several gaps emerged. These were in the detective and reactive clauses of the RTPs. However, they were straightforward to fill using custom controls (see ISO/IEC 27003 for a discussion on custom controls). Only 12 were required, which is not significant. Nevertheless, the exercise demonstrates the power of the ISO/IEC 27002:2022 concept of a custom attributes in helping to create robust RTPs.

USING CONTROL-EVENT SCENARIO MAPPING TO FIND MISSING APPLICABLE RISKS

Since the 12 events used in the previous exercise were designed to ensure coverage of the 114 edition 2 controls, it was natural to ask:

1. What events are required to ensure coverage of the 93 edition 3 controls?
2. In what way do these differ from the edition 2 events?

Some of the new controls in ISO/IEC 27002:2022 deal with risks that have an atypical association with the loss of confidentiality, integrity, and availability. From an organizational perspective,

information is either created or acquired. If information has lost its integrity prior to being acquired (perhaps even at its point of creation as in the case of fake news) it still falls within the remit of ISO/IEC 27001, Clause 6.1.2 c) 1). One of these new controls is 8.23 (web filtering). This control is intended to reduce exposure to malicious content on websites, but it can also be used to reduce exposure to fake news.

The concept of fake news has been newsworthy for several years now and was very much in the minds of some of the experts who encouraged the adoption of this control. Thinking about how one can address this risk, and its relationship to the traditional preservation of C, I, and A, led the author to the concept of poor stewardship of information. Taking that as an event and rearranging and merging the original events led to 9 new events in place of the original 12. The exercise described above using custom attributes was then repeated. This led to the discovery of 8 more gaps, some of which were preventive in nature. Nevertheless, these gaps were readily filled by easy to create custom controls (e.g. fact checking).

Thus, consideration of the purposes of the ISO/IEC 27002:2022 controls can inspire the identification of further applicable risks.

SUMMARY AND CONCLUSIONS

In this short article we have reported on three qualities of ISO/IEC 27002:2022 that assist organizations to go above and beyond that implied by ISO/IEC 27001 Annex A:

- The guidance text, as well as the control text, in ISO/IEC 27002:2022 can help organizations to discover inadvertently omitted necessary controls.

- The ISO/IEC 27002:2022 attribute concept can help organizations identify gaps in their risk treatment plans (which can then be filled using custom controls).

- The control purposes in ISO/IEC 27002:2022 can help organizations to discover overlooked risk scenarios. In the main, risk treatment plans can then be completed using necessary controls that are associated with the controls in ISO/IEC 27002:2022, but any gaps that arise can be filled by custom controls.

These are valuable added benefits of ISO/IEC 27002:2022, over and above those promised by the standard in its introduction.

INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS

Cesare GALLOTTI (SC 27/WG 1 and Italian expert - cesaregallotti@cesaregallotti.it)

ISO/IEC 27002:2022 control 5.9 has title "Inventory of information and other associated assets". It is usually known as the "Asset inventory" control.

All best practices for information security, quality and service management require to maintain an inventory of resources to protect and control.

The goal of the control is easy to understand: it is not possible to protect and control things you don't know. It is in chapter 5 of ISO/IEC 27002:2022. This means that it is not a technological control, but an organizational one. In fact, the asset inventory includes, but is not limited to, ICT assets.

WHAT THE ASSET INVENTORY SHOULD INCLUDE

The "asset inventory" can be a "set of asset inventories", as stated by the ISO/IEC 27002 itself. In fact, if we need an useful inventory, it cannot be a single one.

The set of inventories can include:

- the information managed by the organization; this inventory can be in quality management system documented information, in static tables or in the process and workflow descriptions; in some cases, this inventory is integrated with the records of processing activities, required by some legislations (e.g. for the personal data protection);

- the devices assigned to employees (in many cases, there are two inventories: one of laptops and desktop pcs and one of smartphones and tablets); these inventories are usually on static tables when used for logging the assignment and the retirement of such devices and on automation tools (e.g. MDM, mobile device management) when used for the update and maintenance of such devices;
- the physical and virtual servers and network devices; these inventories are needed for controlling the status of updates and security functions (access control, antimalware, deletion in case of loss or theft, etc.); nowadays these inventories are usually dynamic and in tools for the network monitoring, the VM management and the patch distribution;
- the employees; this inventory is usually on network directories and on tools for the management of authorizations, roles, competence and payroll;
- the equipment necessary for the good functioning of the ICT devices (e.g. air conditioning pumps and splitters, UPS, batteries, generators); this inventory is usually on static tables or on a BMS (building management system), used for the facility management;
- the physical archives for information on paper or photos; this inventory is usually on maps or static tables, and can be integrated with the inventory of physical keys.

Some organizations can have other inventories, according to their needs.

Information and associated assets should be linked each other. I.e. for each piece of information, the assets used for creating, changing and processing it should be identified. This can be done with a software tool or with static tables and can be part of the inventory of the information.

A very simple example is the following one:

Business process	Information	Process owner	Systems used
Sales	- Agreements with customers.	- Sales.	- File server (Office files); - Email; - Paper archives in sales offices in all sites.
Operations - Scheduling	- Scheduling.	- Planning	- File server (Office files); - Email; - Competence management tool; - Paper archives. - Timetable of employees.
Subcontractor handling	- Subcontractor contracts.	Finance	- File server (Office files); - Email; - Competence management tool; - Paper archives. - Accountability system.
Invoicing - Customers	- Accountability books; - Invoices; - Credit monitoring; - Statements of receipt.	Finance	Systems for all: - File server (Office files); - Email; - Accountability system; - Paper archives.
HR - Competence and Qualification	- CVs; - Certificates of competence; - Training needs.	HR	- File server (Office files); - Email; - Accountability system; - Paper archives.
...	...	...	...

For devices and infrastructure components and equipment, an additional inventory should link each component (or group of components) to the relevant suppliers, used for the acquisition and maintenance of the device, component or piece of equipment.

It is needed to periodically verify the correctness of the inventories (especially if they are static). For example, many times it is possible to find in the directories of employees the names of people that left the organization or, in the list of personal devices, items that have been retired and destroyed. The verification helps for the maintenance of the trustworthiness of the inventories and for identifying improvements for the process followed for the addition, change and deletion of the inventory items.

THE LEVEL OF DETAIL

The ISO/IEC 27002 is clear: “the granularity of the inventory should be at a level appropriate for the needs of the organization”. This means that the level of detail depends on the established objectives. Meaningful objectives include traceability in case of loss of theft, the control of software updates, the configuration of authorizations, the incident response and recovery planning.

An example for personal devices: for an organization that provides payroll services, it is usually a good measure to list all devices and their serial numbers; for an organization that provides wiretapping services to judicial authorities, the inventory should also include the RAM and hard disk serial numbers.

Too many data don’t help. If the creation and maintenance of the inventories require too much work for achieving the objectives, they eventually are not effectively updated, then become useless.

ASSET INVENTORY, CMDB AND CMS

In service management, mainly in ITIL, the term “Configuration management database” or “CMDB” is used. This database includes the assets that contribute to the service: pcs and other

personal devices, servers, IT applications, middleware, users, equipment, etc. The difference between the "asset inventory" and the "CMDB" is that in the latter all items must be linked to one or more services.

In 2007, ITILv3 used a new term: "Configuration management system" or "CMS", i.e. a federation of CMDBs. This is because the authors recognized the impossibility to have only one database.

The asset inventory does not need to have assets linked to the relevant services. Nevertheless, CMDBs and CMS can be used as asset inventories.

INVENTORY AND RISK ASSESSMENT

The risk assessment should obviously consider the assets used for managing information, but does not need to have a risk assessment for each asset.

Nevertheless, each asset should be classified, according to a classification scheme. This scheme does not need to be unique: there can be a classification scheme for information (e.g. with labels "secret", "top secret"), for ICT assets (e.g. with labels "critical" or "not critical") and for physical archives (e.g. with labels "sensitive data" or "non-sensitive data").

ISO/IEC 27002 leaves room for each organization to choose the most suitable and effective classification scheme.

OWNERSHIP OF ASSETS

The control 5.9 of ISO/IEC 27002:2022 merges two controls of ISO/IEC 27002:2013: the 8.1.1 (Inventory of assets) and the 8.1.2 (Ownership of assets).

Both standards say that each asset should be assigned to an individual or a group or a function. This means that, for example, production servers can be owned by the "IT Operation" function, not by a specific individual, while personal devices (laptops, smartphones, etc.) can have an owner (e.g. the IT department, with the responsibility of the configuration and update) and a custodian (e.g. the employee that uses them).

The asset owner has the responsibility to ensure that:

- the asset is inventoried in the relevant inventories;
- the asset is appropriately classified and protected;
- the rules for the acceptable use of the assets are established;
- the access restrictions are consistent with the asset classification and and regularly reviewed;
- the deletion or disposal of the asset are securely handled;
- the asset is considered in the relevant risk management activities.

STORAGE SECURITY AND ISO/IEC 27002

Eric Hibbard (editor of ISO/IEC 27040 and US expert)

BACKGROUND ON ISO STORAGE SECURITY

The first edition of the ISO standard on storage security was published as ISO/IEC 27040:2015, *Information technology – Security techniques – Storage security*. This standard provided specific, security-related guidance for storage systems and ecosystems, including products and services, as well as for protection of data in these systems. It was written to be relevant to commercial, government, and non-profit institutions of almost all sizes with operations ranging from a single site to multi-national deployments. The standard also helped organizations identify their existing storage infrastructures, prioritise implementation of security controls by criticality to the organization's business and mission, and articulate the risks related to storage systems and infrastructures.

As originally envisioned, storage networking would have been addressed as an additional part of the ISO/IEC 27033 (*Information technology – Network security*) multi-part standard. However, ISO/IEC 27033 explicitly excluded storage network from its scope and storage security issues were much broader than just storage networking. As such, the decision was made to address the full range of storage security issues within a standard on the topic. The ISO/IEC 27033 roots, however, had a major impact on the structure and focus of the ISO/IEC 27040:2015 standard, which included:

- Storage security overview and concepts (modelled on ISO/IEC 27033-1)

- Guidelines for the design and implementation of storage security (modelled on ISO/IEC 27033-2)
- Storage security threats (modelled on ISO/IEC 27033-3)

IMPACT OF ISO/IEC 27002:2022 ON ISO/IEC 27040

When ISO/IEC 27001:2013 and ISO/IEC 27002:2013 were being drafted, the ISO/IEC 27040 project was in very early stages of development and not referencable. However, these standards did include topics that were relevant to storage security (e.g. storage media handling and backups). These topics were identified and explicitly noted in the ISO/IEC 27040:2015 standard, providing a linkage to these important information security management systems (ISMS) standards. Efforts were also made to avoid duplicating controls covered in ISO/IEC 27002:2013 that were relevant and not unique to storage security.

These early efforts to identify storage security topics within ISO/IEC 27002 became important during the development of what has now become ISO/IEC 27002:2022. This new edition of ISO/IEC 27002 identifies ISO/IEC 27040 as a source of additional information and controls for information backup and sanitising storage media. With this linkage established between ISO/IEC 27002 and ISO/IEC 27040, special attention can be paid to these topics in future revisions of ISO/IEC 27040.

At the time of this writing, ISO/IEC 27040 is undergoing revision and is at the Draft International Standard (DIS) stage. The scope of ISO/IEC 27040 has been expanded to include requirements, which help establish a baseline set of storage security controls that should be considered. Another major aspect of this revision is to update the elements of storage covered by this standard and to reflect the current state of storage security technologies and practices.

The impact of ISO/IEC 27002:2022 on this new edition of ISO/IEC 27040 is significant and includes:

- The ISO/IEC 27002 structure based on the control themes of organizational controls, people controls, physical controls, and technological controls has been adopted in ISO/IEC 27040. The original structure that was modelled on ISO/IEC 27033 has been abandoned.
- In each of the new ISO/IEC 27040 control clauses, a summary of the ISO/IEC 27002 controls is provided along with a declaration that the listed ISO/IEC 27002 controls are relevant to storage systems and ecosystems.
- Controls within ISO/IEC 27002:2022 that have a potential storage component have expanded coverage in the new ISO/IEC 27040.
- ISO/IEC 27040 now includes requirements associated with storage sanitisation (both logical and media-based). The media-specific sanitisation techniques (i.e. how to sanitise specific types of storage devices and media) has be deferred to the new IEEE 2883 *Standard for Sanitizing Storage*, which represents the current state of storage technology and it can be updated as needed without impacts to ISO/IEC 27002 or ISO/IEC 27040.
- The ISO/IEC 27002:2022 use of attributes to facilitate different views or categorizations of the controls influenced the inclusion of labels for controls or clusters of controls in ISO/IEC 27040 that can help an organization identify the most relevant storage security controls.

ANTICIPATED FOCUS OF ISO/IEC 27040 (2ND EDITION)

As a part of the ISO/IEC 27000-series family of standards, the second edition of ISO/IEC 27040 is expected to provide specialized requirements and guidance associated with:

- storage system security hardening;
- secure management of storage;
- data at rest encryption for storage;
- data in motion protections for storage;
- key management services;
- storage sanitisation;
- storage networking security;
- block, file, and objected-based security;
- cloud storage security;
- data protection and recovery;
- securing data archives and repositories;
- storage virtualization security;
- secure multi-tenancy; and
- secure autonomous data movement.

This new version of ISO/IEC 27040 is projected to be published in late 2022 or early 2023.

In conclusion, ISO/IEC 2702:2022 has enhanced visibility of storage security issues with some key references to ISO/IEC 27040. This situation is anticipated to improve significantly with the publication of the new edition of ISO/IEC 27040, which has a much closer alignment with ISO/IEC 27002.

INTRODUCING THE NEW CONTROL ON CLOUD SECURITY IN ISO/IEC 27002

Benoit Heynderickx
Principal Analyst at the Information Security Forum

INTRODUCTION

The latest ISO/IEC 27002 introduces 11 new controls and one of them, control 5.23, advocates the secure use of cloud services.

This article examines this noticeable addition and explores some important questions that users may ask themselves when it comes to cloud security and control 5.23:

- Is there really a need for a new cloud security control?
- What are the most important aspects of the new control 5.23?
- Are there any other important considerations when implementing the control?
- In summary, how should my organisation implement the new control 5.23 for securing the use of cloud services?

THE NEED FOR CLOUD SECURITY CONTROLS

The technology landscape has evolved tremendously since the 2013 version of ISO/IEC 27002, and whilst cloud computing was already in existence, cloud security controls were not directly mentioned in the previous standard. Cloud security related controls were covered either in the supply chain controls of ISO/IEC 27002:2013 (15.1 Information security in supplier

relationships) and subsequently in ISO/IEC 27017:2015 and ISO/IEC 27036-4: 2016.

In the meantime, global cloud infrastructure spend has increased nearly 13-fold from 2012 to 2022: from around $10bn in 2012 compared to $130bn in 2020. Organisations now spend more on cloud infrastructure than they do on in-house data centres (Synergy, 2020).

ISF research highlighted the need for organisations that have recently acquired a multitude of cloud services to be extremely vigilant when deploying their applications:

> "Cloud security is not the sole responsibility of the cloud service providers, it is mostly incumbent on the cloud customer, especially for those using IaaS and PaaS type services." (ISF, 2019)

The new ISO/IEC 27002 control 5.23 is therefore a welcome addition and will help organisations strengthen their usage of the multitude of recently acquired cloud services.

EXPLAINING THE NEW ISO/IEC 27002 CONTROL 5.23

The newly introduced control defines some best practices to apply throughout the lifecycle of cloud services used by an organisation. The control considers the acquisition, usage, management and termination of cloud services. It primarily considers cloud security from a cloud service customer perspective.

The control gives more detailed guidance for practical implementation with a focus on:

- The role of a cloud service customer (the organisation that is the acquirer of cloud services) in planning and deploying the necessary information security requirements over its cloud service provider(s) with the need to have in place;
    - A policy statement for the use of cloud services, which can be an extension of an existing information security policy,
    - A scoping statement detailing which cloud services are in use and their key characteristics (similar to an inventory of cloud services),
    - A risk assessment to determine the necessary controls to deploy for the secure use of cloud services,
    - A set of information controls to manage risks over cloud services (using some of the controls described in ISO/IEC 27002 or referring to other standards such as ISO/IEC 27017),
    - a strong monitoring capability for the existing use of cloud services,
    - a clear exit strategy, should the organisation wish to terminate the relation with the cloud service provider,
- The need to firm up the contract clauses or the agreement between the cloud service provider and the acquiring organisation, highlighting that such agreements can sometimes be difficult to negotiate;
- The specific requirement for controlling significant changes being made by the cloud service provider such as a change of location or change of infrastructure.

Cloud services can vary in form and shape and therefore the control highlights the importance of understanding the concept of shared responsibility between the cloud service customer and the cloud service provider. The shared responsibility for information security is an overarching principle for reading and implementing this control.

The successful implementation of ISO/IEC 27002 control 5.23 also requires a good understanding of some important additional considerations such as cloud computing characteristics, supplier relationships and which security control framework to apply.

IMPORTANT ADDITIONAL CONSIDERATIONS WHEN IMPLEMENTING CONTROL 5.23

a) Cloud computing characteristics

Cloud computing has some intrinsic features which have been defined in the ISO/IEC 17788 : "(Cloud computing enables) network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand."

The description of ISO/IEC 27002 control 5.23 mentions the importance of understanding the shared responsibilities between customers and providers and therefore organisations must be cognisant of the types of cloud services that they are using. Levels of responsibilities between cloud service providers and customers differ across the three main cloud service models described in the table below:

Cloud service Model (ISF, 2019)	
infrastructure as a service (IaaS)	Covers the physical hosting of the servers and all necessary computing resources as well as backend services, such as hardware and networking capabilities.
platform as a service (PAAS)	Adds more services such as an operating system, software-defined networking and middleware in addition to the IaaS services provided.
Software as a service (SAAS)	Delivers fully functioning business applications that include the underlying infrastructure, networking and middleware, which can often be customised to meet organisational needs, sometimes altering some of the built-in application logic.

Cloud service customers are typically responsible for more controls than their cloud service providers when using IaaS with responsibilities for areas such as network virtualisation, secure configuration, data protection and access management. Whereas when using SaaS, cloud service customers will look after a smaller subset of controls such as access management and data protection only.

When scoping cloud services, it is also important to categorise them according to the type of deployment, such as described in the table below:

Cloud Deployment Model (ISF, 2019)	
public cloud	Cloud services available to purchase by the general public over a public network, typically the internet (the most common type of cloud deployment).
private cloud	Comprised of one or more cloud services deployed for the exclusive use of a single organisation; typically managed by an external provider of IT services and often accessed over a restricted network.
hybrid cloud	A combination of both private and public cloud.

The levels of controls offered by the public cloud service providers are typically described in the contractual arrangements and can also be publicly accessible, especially for the largest cloud service providers. There is usually little room for control alterations with public cloud, whereas organisations choosing to deploy a private cloud environment will have more leverage in negotiating the types of controls they want their provider to deploy.

Cloud characteristics should be well documented in cloud inventories, including mention of the types of cloud service (IaaS, PaaS, SaaS) and cloud deployment model (Public, Private, Hybrid) in use.

b) Supply chain controls

The ISO/IEC 27002 controls on supplier relationships (5.19), supplier evaluation (5.20) and contract monitoring (5.22). Cloud service providers should in this sense be treated as another supplier and the necessary due diligence and contractual reviews when acquiring new could services.

Example: **5.19 Information security in supplier relationships**

"This (control) should also apply to the organization's use of resources of cloud service providers."

Meanwhile there are some specific aspects to managing the equivalent of a full-scale data centre with a cloud infrastructure, which often is fragmented across multiple cloud providers (e.g. understanding of the cloud service model and cloud deployment model, the need for broad network access, the management of a shared and elastic pool of resources).

Supply chain controls should therefore be looked at when considering the use of cloud services, but cannot and should not supersede the specific control on use of cloud services.

c) Security control frameworks that can be applied for cloud security

To meet the new control guidance on the need to deploy a series of information security controls over their cloud services, organisations can look at other international information security frameworks. The most noticeable ones are:

- ISO/IEC 27017:2015

The standard takes the ISO/IEC 27002 (in its 2013 version) and provides guidance on how to apply the controls in a cloud-based environment for both cloud service customers and providers. It therefore refers to the previous version of the security controls, which might be problematic for organisations keen to deploy the latest version of the ISO/IEC 27002:2022. An updated version will soon follow and is currently under revision with the SC 27 currently working collaboratively with ITU-T on ITU X.1631 | ISO/IEC 27017.

ISO/IEC 27018:2019 can also be used for deploying security controls for cloud services specifically for those organisations storing PII in their cloud environments.

- ISO/IEC 27036-4:2016

The standard was published as the fourth part of ISO/IEC 27036 which covers a broad spectrum of information security guidelines for supplier relationships. ISO/IEC 27036-4 is focused on a specific aspect of supplier relationships, namely cloud computing, and how organisations should assess their risks specific to their acquisition and use of cloud services.

- Cloud Security Alliance (CSA): Cloud Controls Matrix (CCM) version 4

The CSA first published its library of cloud controls in 2010 with version 1 of the cloud controls matrix. In its latest version 4, the list contains 197 control objectives that are applicable for both

cloud service customers and cloud service providers. The control catalogue accommodates for a full list of security controls typically deployed for cloud services.

- Information Security Forum (ISF), Using Cloud Services Securely (2019)

The ISF published a comprehensive guide for deploying a series of core security controls aided by cloud security governance and the effective use of cloud security products. The list of 45 controls gives a foundation for some of the most important areas for using cloud services securely. It can also be complemented by more detailed controls libraries such as the one provided in the Standard of Good Practice for Information Security (ISF, 2020).

- Centre for Internet Security (CIS) Critical Security Controls Version 8

The CIS has published an updated list of security controls, enhanced to support organisations' security control frameworks when moving to cloud computing. It comprises 18 high-level controls further divided into 153 'safeguards', all aimed at securing a complete environment. There is also the recent addition of Control 15: Service Provider Management, which specifically aims to look after external suppliers such as cloud services providers.

- National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1

The popular framework from NIST can be applied for the use of cloud services partially or in its entirety. It also covers specific content on supplier chain risk management (ID.SC) with an indirect coverage of cloud services.

Some of the above mentioned information security standards cover cloud security in its entirety such (e.g. the CSA CCM), whereas other international standards treat cloud security as one aspect of a wider security control environment (e.g. ISF SOGP, CIS, NIST and now ISO/IEC 27002).

HOW-TO IMPLEMENT CONTROL THE NEW ISO/IEC 27002 CONTROL 5.23 EFFECTIVELY

Organisations want to manage their cloud services effectively and securely, and to help them the new ISO/IEC27002 has introduced a new control 5.23. Whilst it cannot be used in isolation, it gives a good basis (or a starting point) for risk assessing and controlling their use of cloud services. In summary it is important for organisations to apply the following:

1. Read the full control to get a good understanding of some of its most important aspects:
    - The control applies primarily for organisations acting as cloud service customer
    - The control involves the understanding of the shared responsibility between cloud service customer and cloud service provider
    - The control requires the scoping of cloud usage; it is necessary to perform an inventory of all cloud services and document the main characteristics of each one.
2. Grasp the main control guidance especially on:
    - The need to write and distribute a policy on the use of cloud services
    - The need to determine a set of security controls based upon another external information security control library (and it can be based upon part or all of ISO/IEC 27002)

- The need to perform the necessary supplier due diligence and contractual reviews (see also control 5.20 Addressing information security within supplier agreements).

3. Use additional material such as:
   - ISO/IEC 17788 to gain an understanding of the fundamental cloud characteristics
   - ISO 27017 for deploying and reviewing cloud specific controls
   - ISO/IEC 27036-4 for the risk assessment of acquisition and use of cloud services
   - Other international security standards such as CSA, ISF, CIS or NIST.
4. Select the necessary controls for the secure use of cloud services and validate the approach.

Cloud computing is constantly evolving and organisations are now spending most of their IT budget in cloud computing technologies, so now is the time to embrace cloud security.

REFERENCES

(A) Centre for Internet Security (CIS), CIS Critical Security Controls Version 8, 2021, Available at https://www.cisecurity.org/controls/v8

(B) Cloud Security Alliance, Cloud Controls Matrix Version 4, July 2021, Available at https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

(C) Information Security Forum (ISF). Using Cloud Services Securely – Harnessing core controls, November 2019, Available at https://www.securityforum.org/solutions-and-insights/using-cloud-services-securely-harnessing-core-controls/

(D) Information Security Forum (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2020. Available at https://www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/

(E) Synergy Research Group, 2020—The Year That Cloud Service Revenues Finally Dwarfed Enterprise Spending on Data Centers, 18 March 2021, Available at https://www.srgresearch.com/articles/2020-the-year-that-cloud-service-revenues-finally-dwarfed-enterprise-spending-on-data-centers

(F) ISO/IEC 17788:2014, Information technology — Cloud computing — Overview and vocabulary

(G) ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls

(H) ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

(I) ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

(J) National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, Available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

HALL OF FAME

The development of ISO/IEC 27002 was managed by Edward HUMPHREYS (WG 1 convenor). The editors for the 3rd edition were Sabrina FENG (GB), Alia FOURATI (FR), Veronica MARINELLI (AR). The following is a list experts that made contributions to the development of working documents for the 3rd edition of ISO/IEC 27002.

AGARWALA, Sanjiv (IN)
ALLARD, Jean-Luc (BE)
ANDERSSON, Anna (SE)
ARIFFIN, Azleyna (MY)
BARTOL Nadya (US)
BLAKE, Derek (GB)
BLIX, Fredrik (SE)
BRANZELL, Jan (SE)
BREWER, David (GB)
CASTEEL, Erin (AU)
DICKMAN, Peter (CH)
EDWARDS, Mike (GB)
FARIAS, Ariosto (BR)
GALLOTTI, Cesare (IT)
GUASCONI, Fabio (IT)
IWAMOTO, Kazunori (JP)
JALALUDDIN, Abu Arif (MY)
JAMES, Dawn (GB)
KIKUCHI, Masato (GB)
Königs, Hans-Peter (CH)
Krzyzewski, Tony (NZ)
LINDE, Anders (DK)
LINDSAY, Laura (US)
LUCY, Kimberly (US)
MARINELLI, Veronica (AR)
MIN, Jinghua (CN)
NAGAMIYA, Tadashi (JP)
OLSEN, Rainer (CH)
PATEL, Milan (GB)
POOLE, Vernon (GB)
ROBINSON, Gigi (GB)
Sakimura, Natsuhiko (OECD)
Sasseville, Pierre (CA, ISACA)
Söderlund, Lars (SE)
SOLAND, Marcus (CH)
SNARE, John (AU)
Søndenaa, Are (NO)
Starkerud, Kristina
SUO, Amanda (ES)
SUZUKI, Toshimitsu (JP)
TAKEDA, Eisaku (JP)
Tsuchiya, Naoko (JP)
Vandenbranden, Geert (BE)
WATKINS, Steve (GB)
WEBER, Reto (CH)
WEISS, Peter (CH)
YAMASHITA, Shin (JP)
Yeomans, Michael (ISF)
ZHANG, Jian (CN)
ZAMORA, François (FR)
Åhlfeldt/IIT, Rose-Mharie (SE)

Country codes: Argentina (AR), Australia AU), Belgium (BE), Brazil (BR), Canada (CA), China (CN), Denmark (DK), France (FR), India (IN), Italy (IT), Japan (JP), Malaysia (MY), New Zealand (NZ), Norway (N), Spain (ES), Sweden (SE), Switzerland (CH), United Kingdom (GB), United States (US).

The following is a list National Standards Bodies that made contributions to the development of CD and DIS text for the 3rd edition of ISO/IEC 27002:

Australia (SA)
Austria (ASI)
Belgium (NBN)
Brazil (ABNT)
Canada (SCC)
China (SAC)
Cyprus (CYS)
Denmark (DS)
Estonia (EVS)
Finland (SFS)
France (AFNOR)
Germany (DIN)
India (BIS)
Ireland (NSAI)
Italy (UNI)
Japan (JISC)
Kenya (KEBS)
Korea (KATS)
Luxembourg (ILNAS)
Malaysia (DSM)
Mexico (DGN)
Netherlands (NEN)
New Zealand (NZSO)
Norway (SN)
Poland (PKN)
Russian Federation (GOST R)
Singapore (SSC)
South Africa (SABS)
Spain (UNE)
Sweden (SIS)
Switzerland (SNV)
United Kingdom (BSI)
United States (ANSI)

Thirty-three countries were involved in the development of ISO/IEC 27002:2022

AUTHOR BIOS

Dr Andreas WOLF

Dr. Andreas Wolf studied mathematics and computer science at Humboldt University in Berlin and Technical University Munich, where he received his doctorate in computer science in 1999. In his dissertation, he dealt with parallel automated reasoning, a special aspect of artificial intelligence. In the past, he worked in technology-oriented positions with IT companies in Munich, Jena and Berlin, focusing on IT security and in particular on biometric technologies. He initiated the first European certification of a product for biometric speaker recognition according to Common Criteria. Today Dr. Wolf works as Principal Scientist Biometrics with Bundesdruckerei GmbH, Berlin. He has published several book and journal contributions as well as conference papers and received more than 30 patents. He teaches applied biometrics at the Institute for Mathematics and Computer Science of the Free University of Berlin. He is one of the German DIN experts delegated to the ISO/IEC JTC 1 committees SC 17, SC 27, SC 31 and SC 37 and to the European standardization committee CEN/TC 224. He is chairman of ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and data protection", convenor of CEN/TC 224/WG 19 "Breeder documents" and editor or co-editor of several standards, including the ICAO Technical Report on Portrait Quality and the biometric face image data formats ISO/IEC 19794-5/39794-5 which are used in all electronic ID documents

Dr Edward HUMPHREYS

Dr Edward Humphreys started working on ISO security standards in 1982, during this time he has managed several standards groups including SC 27/WG 1, which he still leads, and directs the development and maintenance of the ISO/IEC 27000 family of

standards. He also the managed the development of the UK ISMS standards BS 7799-1 and -2, the forerunners of ISO/IEC 27002 and ISO/IEC 27001, and the ISMS accreditation standard EA 7/03 9 (now ISO/OEC 27006). He has over forty years business experience in information and IT security. He is a professor at several universities and is the author of seven books on information and cybersecurity.

Sabrina FENG

Sabrina is an experienced leader in technology, cyber, resilience and risk. She currently holds the position of Head of Technology, Cyber and Resilience Risk at the London Stock Exchange Group (LSEG). Prior to joining LSEG in January 2019, Sabrina was Group CISO for four years, at Equiniti, where she set up and matured its Group Security function and delivered the cybersecurity transformation programme. Prior to that she held senior roles at AXA Group and VISA EMEA managing Security and Risk.

She actively participates in ISO standard drafting activities since 2011, currently serving as Vice Chair of IST33/1, the UK Mirror Committee of ISO/IEC SC27/WG1, and the Editor of 27002:2022. She is a guest lecturer for the MSc in Information Security at Royal Holloway, University of London, also an external member of the Audit committee at The London School of Economics and Political Science. Sabrina has an MSc. Information Security from Royal Holloway, University of London.

Alia FOURATI

Alia Fourati received a Master's degree in Computer Science and a Postgraduate degree on "Réseaux et Télécoms" from INSA Toulouse, respectively in 1999 and 2000. She then obtained a PhD degree in Computer Science from Université Paul Sabatier (Toulouse, France) and then was Post-doc from 2005 to 2007 at the LRI Laboratory (Paris-SUD XI University, France). Both PhD and

Post-doc research addressed information security. She joined EDF R&D in 2007 as a researcher-engineer in cybersecurity. Among its activities, Alia is involved in international and European standardization in cybersecurity (member of ISO/IEC JTC1 SC27, CEN-CLC JTC 13, IEC ACSEC). She has been co-editor of ISO/IEC 27019:2017 "Information security controls for the energy utility industry" and of the revision of ISO/IEC 27002:2022 " Information security controls".

Veronica MARINELLI

Verónica Marinelli is a chemist (Licenciada en Ciencias Químicas, UBA) and specialises in information security. She has over 12 years of experience in the field of information security, working on PKI, digital signature, development of standards for CAs certification procedures, validation, issuance and management procedures for digital certificates and other PKI related agreements. For the last 11 years she has worked as standardization project manager at IRAM (Instituto Argentino de Normalización y Certificación). She was co-editor of ISO/IEC 27002:2022.

Jan BRANZELL

Jan Branzell is CEO at Veriscan Security AB and started working with standardization in year 2000 in the Swedish mirror committee. He joined SC 27 in 2003 and later became editor for ISOIEC 27003:2010- “implementation guidance” and the 2017 edition that focused just on guidance on ISO/IEC 27001, and also among others editor for ISO/IEC 2016:2014 on information security management economics. Jan has over the years provided many contributions to standardization based upon practical experience on how organizations ranging from 10- 100, 000 employees benefits from using the ISO 27000 series of standards.

Dr David BREWER

Dr David Brewer is a director of IMS-Smart Limited. He has over 35 years' worldwide experience working with management systems as a standards maker, consultant, auditor, tutor, and integrated management system administrator. He was involved with the development of the original ISMS standards, BS7799 Part 1 and Part 2, and is an active member of ISO/IEC JTC 1 SC27 WG1. He has conducted a wide variety of information security consultancy assignments in over 23 countries. His seminal research papers include: The Chinese Wall Security Policy, published in 1989; and Measuring the Effectiveness of an Internal Control System, published in 2003.

Cesare GALLOTTI

Cesare Gallotti has been an information security, privacy, quality, service management and business continuity consultant since 1999. He also carries on audits (of first, second and third party) and designs and delivers training sessions on the same subjects.

He published the book "Information security" (last edition in 2022). Since 2008 he has delivered a newsletter on the subjects above (https://www.cesaregallotti.it/Newsletter.html and on LinkedIn) in Italian and, since 2022, English. He has worked, as Italian expert, in the ISO/IEC JTC 1 SC 27 WG 1 and WG 5 for the standards ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27701 and others.

Eric HIBBARD

Eric A. Hibbard is the Director, Product Planning – Storage Networking & Security at Samsung Semiconductor, Inc. and a cybersecurity and privacy leader with extensive experience in industry, U.S. Government, and academia.

Mr. Hibbard serves in leadership positions in standards development organization and industry associations, including the InterNational Committee for Information Technology Standards (INCITS), the IEEE Computer Society, the American Bar Association, the Cloud Security Alliance, and the Storage Networking Industry Association. Hibbard is or has served in an editorship role on the ISO/IEC 22123 (Cloud computing), ISO/IEC 27050 (Electronic discovery), ISO/IEC 27040 (Storage security), ISO/IEC PAS 20648 (TLS for storage systems), Rec. ITU-T 3500 | ISO/IEC 17788 (Cloud computing -- Overview and vocabulary), and IEEE 1619-2018 (XTS-AES).

Mr. Hibbard possesses professional credentials that include the (ISC)2 CISSP-ISSAP, ISSMP, and ISSEP certifications; IAPP CIPP/US and CIPT certifications; ISACA CISA and CDPSE certifications; and CSA CCSK certification. He has a BS in Computer Science.

Benoit HEYNDERICKX

Benoit is a Principal Analyst at the ISF specialising in supply chain, cloud security and quantitative risk analysis.

As experienced information security professional, he has a wealth of knowledge and practical experience implementing large scale information security and risk programmes such as ISMS, SOX IT Compliance, and third-party risk assurance programmes. Benoit holds security certifications from ISACA and the CSA, as well as an MSc in Information Security and Risk from City, University of London. Benoit is also a Full Member of the Chartered Institute of Information Security.