GIS Odyssey Journal

2022 • Volume 2 • Number 2

https://doi.org/10.57599/gisoj.2022.2.2.79

Jerzy Stanik[1], Maciej Kiedrowicz[2]

STATEMENT OF APPLICABILITY AS A KEY ELEMENT OF THE GIS CERTIFICATION PROCESS IN THE LIGHT OF CYBERSECURITY STANDARDS

Abstract: The Statement of Applicability (SoA) is a mandatory document ISMS that you need to develop, prepare, and submit with your ISO 27001, and it is crucial in obtaining your ISO 27001 Risk Assessment and ISMS certification. According to ISO/IEC 27001, Information Security Management System is a collection of 'that part of the general management system, based on the approach to business risk, to establish, implement, operate, monitor, review, maintain and improve information security. ISO/IEC 27001 specifies the requirements and implementation process for the Information Security Management System. However, implementing this standard without a good SoA document may prove impossible. The article presents a system model for the construction of SoA for ISMS and its certification following the ISO 27001 standard. This model aims to provide instruments for designing and generating an SoA document in relation to ISMS, covering all information processes in GIS. This model allows organizations to evaluate their current state of GIS information asset security implementation according to the best practices defined in ISO/IEC 27001. The proprietary model proposed in this article is assessed from a multi-stage perspective, which confirms that the proposed draft Statement of Use document makes a valuable and innovative contribution to information security management by considering the best practices in this field.

Keywords: spatial data, security, Statement of Applicability (SoA), risk, implementation process

Received: 8 June 2022; accepted: 3 August 2022

[1] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland, ORCID ID: 0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl

[2] Military University of Technology, Faculty of Cybernetics, Institute of Computer and Information Systems, Warsaw, Poland, ORCID ID: 0000-0002-4389-0774, email: maciej.kiedrowicz@wat.edu.pl

Introduction

In the era of constantly increasing amounts of spatial data and geodata, which are the pillar of each GIS class system, it is necessary to ensure appropriate organizational and technical security mechanisms, as it is of key importance for the effectiveness of each system.

Observing the regulatory changes in the European Union and the world in the area of GIS and cybersecurity, one can notice a significant increase in the requirements for the security mechanisms used – legal, organizational and technical safeguards – in information security management systems. This is reflected in the requirements of new standards and regulations, such as standards in the field of information security management – ISO/IEC 27001, the General Data Protection Regulation (GDPR) (EU) 2016/679, or the new cybersecurity directive (EU) 2016/1148. This fact also influences the preparation of the declaration of use and forces the improvement of current solutions in terms of their structure. A well-drafted declaration of use must correctly reflect the selection of safeguards and protects against the potential risk.

In the era of cybersecurity, the design and implementation of adequate security systems concerning information processes in GIS are very important, especially when we want to obtain a security certificate for GIS. Thanks to the flexibility in selecting a set of organizational and technical security measures and their innovative solutions, each GIS-class system can be made professional from the point of view of cybersecurity.

Two types of goals are distinguished in the work: cognitive and practical. The cognitive goal of the presented research is to gain multifaceted knowledge about the currently existing document templates entitled 'SoA' for ISMS certification and for compliance with the ISO/IEC 27001 standard, with particular emphasis on its effectiveness, correctness and conditions. The practical goal is to develop an SoA pattern/project and indications and conclusions for employees of the security department to properly apply this pattern in the construction of the Information Security Management System for compliance with the ISO/IEC 27001 standard. The auxiliary goals are (Al-Mayahi and Mansoor, 2008; Chi-Chun and Wan-Jia, 2012):

1) reviewing the current state of knowledge in Poland on the currently existing templates of the document entitled 'Statement of Use' for the certification of the Information Security Management System for compliance with the ISO/IEC 27001 standard,
2) assessment of its impact on the manner and effectiveness of the certification process,
3) making a comparative analysis of these patterns and presenting own comments, recommendations, suggestions or recommendations for their improvement.

In terms of content, the article addresses the following problems (web pages: www.pcisecuritystandards.org, www.sans.org, nvlpubs.nist.gov):

- Problem 1. The SoA cannot be built without a clearly defined ISMS scope.
- Problem 2. The utility of an SoA depends significantly on the current risk analysis results concerning the established set of information resources to be protected.

- Problem 3. The most desirable SoA is one that should refer to all 18 groups of security application targets listed in Annex A of ISO/IEC 27001. In addition, for each target (114 targets in total), rules, documents, and responsible persons must be specified.

The problems mentioned above constitute the main threads of the final work and determine its framework. This article presented the SoA draft document and the tools and instruments enabling its development were developed based on available literature and own research.

Statement of Applicability and its development process

Statement of Applicability. The Statement of Applicability (SoA) is a central, mandatory part of the ISO 27001 standard for Information Security Management Systems (ISMS). The information security management system focuses on continuous improvement and the declaration of use document helps you to achieve this.

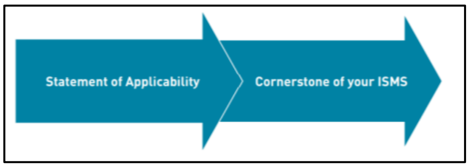


Fig. 1. Linking the SoA to the ISMS
Source: own elaboration

The Statement of Applicability forms the main link between your risk assessment and the information security you have implemented (Fig. 1). The purpose of the Statement of Applicability is to document which controls (security measures) from ISO 27001 Annex A (and thereby the ISO 27002 standard for information security) you will implement and the reason they have been chosen – as well as justify why any controls might be excluded.

It is also good practice to include the following in the Statement of Applicability document (see: www.neupart.com):

- The status of implementation for existing controls
- A link to the control documentation or a brief description of how each control is implemented
- A cross-reference to the sources of other requirements necessitating the controls chosen.

Thus, by preparing a good quality Statement of Applicability, you will have a thorough and complete overview of which controls you need to implement, why they are implemented, how they are implemented, and how well they are implemented.

The Statement of Applicability results from numerous activities defined in the planning phase of an ISO 27001 implementation. The two primary sources for the Statement of Applicability are the risk assessment and Annex A of the standard – in reality, the Table of Contents of the ISO 27002 standard (see: ISO/IEC 27001:2013; ISO

Standard 27001 and ISO Standard 27002). Other sources are the controls in the organization and external security requirements that the organization has to comply with.

The road to the Statement of Applicability. The general scheme [way to] obtain a good Statement of Applicability for a selected organization is shown in Figure 2.

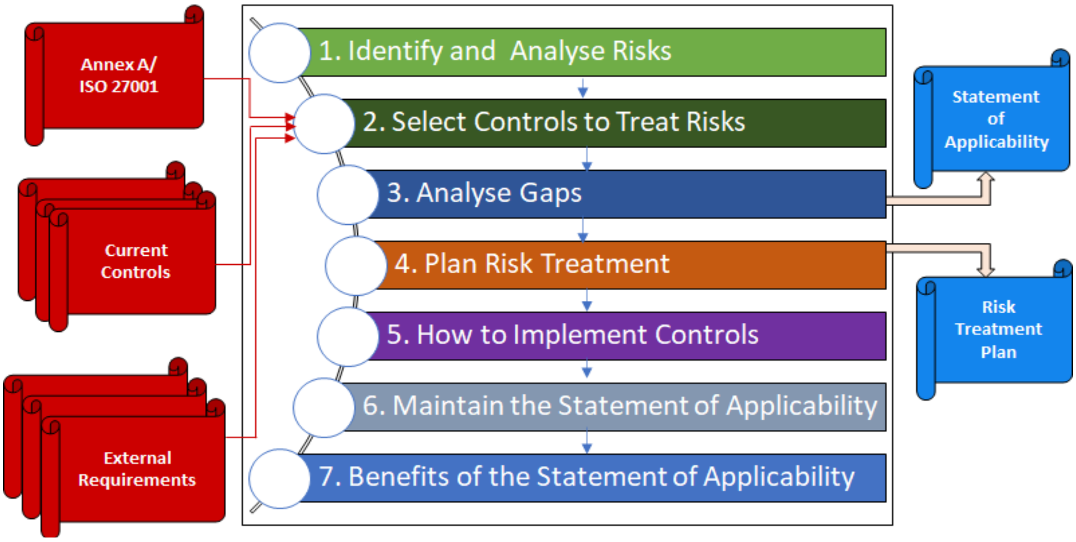

Annex A/ ISO 27001
Current Controls
External Requirements
1. Identify and Analyse Risks
2. Select Controls to Treat Risks
3. Analyse Gaps
4. Plan Risk Treatment
5. How to Implement Controls
6. Maintain the Statement of Applicability
7. Benefits of the Statement of Applicability
Statement of Applicability
Risk Treatment Plan

Fig. 2. The road to the Statement of Applicability
Source: own elaboration

Table 1. A step-by-step process for creating an ISO 27001 Statement of Applicability

Name	General description
Identify and Analyse Risks	To ensure that the implemented controls reflect the risk faced by the organization, a risk analysis should be carried out in two phases: the Identification Phase and the Analysis Phase, and the introduction of elements of good practice. Conduct an ISO 27001 risk assessment by listing all information assets and identifying data security risks for each one. Then, prioritize and prioritize the risk based on probability and impact, assign a risk owner, and create a plan to close any vulnerabilities.
Select Controls to Treat Risks	The analysis has determined that the risks are unacceptable, so proper action must be taken. The risk treatment options are typically: a) Applying appropriate controls b) Knowingly and objectively accepting risks c) Avoiding risks, or: d) Sharing the associated business risks with other parties, e.g. insurers or suppliers. Proper controls must be selected for those risks where option a) above is chosen. Fortunately, ISO 27002 provides us with an excellent catalogue of control objectives and controls for treating risks and good guidance on implementing the controls.
Analyses Gaps	While this is not a strict requirement of the ISO 27001 standard, it is recommended that once the required controls have been selected, a gap analysis is performed to establish the current state of the implementation of the controls.

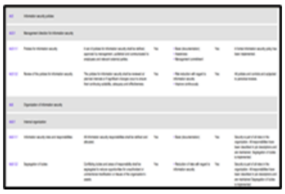
	To ensure the evaluation of the controls is consistent and coherent, it is recommended that a commonly accepted maturity level model be selected. Examples of such maturity scales are: • The COBIT 4.1 Maturity Model • Carnegie Mellon Software Engineering Institute Capability Maturity Model • The Danish Agency for Digitization ISO 27001-benchmark (see: www.digst.dk)
Plan Risk Treatment	As noted in the introduction, the Statement of Applicability is a very central document in the information security management system. After the initial version of the Statement of Applicability has been developed, it will be used both when developing the risk treatment plan and when implementing the controls that have been selected during the 'Select Controls' activity. The risk treatment plan could be said to be the organization's security implementation plan, and the primary goal of the plan is to achieve the organization's security goals.
How to Implement Controls	After the planning of risk management is completed, appropriate protection begins. Depending on how big the difference is between the actual and the necessary levels of security, this can be both a laborious and time-consuming task. Therefore, it is not uncommon for risk management plans to extend over several months or even years. The maturity of the ISMS improves during the implementation of controls and, therefore, the Statement of Use needs to be updated in line with this progress. The Statement of Applicability requires a list of all the controls recommended in Annex A, together with a statement as to whether each control has been applied or not. You must justify each case if you have included or excluded a specific check from Annex A.
Maintain the Statement of Applicability	After selecting the controls and performing a gap analysis of the selected controls, we now have all the information needed to write the Statement of Applicability document. It is recommended to use a structured tool to document the Statement of Applicability. In this way, it will be possible to work with the content of the Statement of Applicability and, for example, sort and filter based on the compliance level, source of requirements and other parameters. Examples of suitable tools to write a Statement of Applicability are spreadsheets, databases and dedicated ISMS tools (www.itgovernance.co.uk, advisera.com).
Benefits of the Statement of Applicability	Here are six reasons why it is an important document to have in your arsenal: 1. Helps you establish eligibility requirements. 2. Provides an overview of crucial information related to the applicant's qualifications. 3. It helps to determine if the applicant meets all the necessary criteria. 4. Document any exceptional circumstances, such as disability-related accommodation. 5. The SoA will be referenced throughout the application process and can sometimes be used as proof of documentation. 6. Finally, it can serve as the basis for some institutions' 'official' letters of good standing.

Source: own elaboration

The Statement of Applicability is one of the first documents an auditor will review as part of the ISO 27001 audit process. The Statement of Applicability helps the auditor understand the organization and what controls have been implemented and assessed as part of that organization's audit.

Comparison table of Statement of Applicability. A schematic illustration of the comparison of selected tools supporting the Statement of Applicability development process is presented in the table below (Table 2).

Table 2. Comparison table of Statement of Applicability

Conformio	ZEBSOFT	ISO 27001 Implementation Kanban Board	Hiperproof
1	2	3	4
Platforms Supported Windows, Mac, Linux SaaS, iPhone, Android	**Platforms Supported** Windows, Mac, Linux SaaS, iPhone, Android	**Platforms Supported** Windows, Mac, Linux SaaS, iPhone, Android	**Platforms Supported** Windows, Mac, Linux SaaS, iPhone, Android
Audience Solutions only for small and medium-sized companies	Audience Organizations that need a Kanban Board that is ISO 27001 compliant	Audience Organizations that need ISO software	Audience Technology companies looking to improve regulatory compliance
Support Work hours 24/7 live support Online	Support Work hours 24/7 live support Online	Support Work hours 24/7 live support Online	Support Work hours 24/7 live support Online
SoA screenshots 	SoA screenshots 	SoA screenshots 	SoA screenshots 
Prices $ 199 a month Free version Free trial version	**Prices** No information available Free version Free trial version	**Prices** No information available Free version Free trial version	**Prices** $ 10,000 per year Free version Free trial version
Training Documentation Webinars Live online Personally	**Training** Documentation Webinars Live online Personally	**Training** Documentation Webinars Live online Personally	**Training** Documentation Webinars Live online Personally
Pieces of information about the company Expert Adviser solutions Established: 2009 Croatia advisera.com	Pieces of information about the company OK Consulting www.okconsultings.com	Pieces of information about the company Established: 2018 Great Britain zebrasoftware.co.uk	Pieces of information about the company Hyper-resistant Established: 2018 United States hyperproof.io

Tool alternatives	Tool alternatives	Tool alternatives	Tool alternatives
VCOMPLY ignyte IMS LTD	VIVIFY scrum KB	Onspring	RiskWatch
Compatibility features Archiving and storage Audit management Compliance Tracking Testing control Compliance with environmental protection requirements FDA compliant HIPAA compliant Incident management ISO compliance OSHA compliant Risk management Polls and opinions Version control Workflow / Automation of processes	**Compatibility features** Archiving and storage Audit management Compliance Tracking Testing control Compliance with environmental protection requirements FDA compliant HIPAA compliant Incident management ISO compliance OSHA compliant Risk management Polls and opinions Version control	**Compatibility features** Archiving and storage Audit management Compliance Tracking Testing control Compliance with environmental protection requirements FDA compliant HIPAA compliant Incident management ISO compliance OSHA compliant Risk management Polls and opinions Version control Workflow / Automation of processes	**Compatibility features** Archiving and storage Audit management Compliance Tracking Testing control Compliance with environmental protection requirements FDA compliant HIPAA compliant Incident management ISO compliance OSHA compliant Risk management Polls and opinions Version control Workflow / Automation of processes

Source: www.itgovernance.co.uk, advisera.com

Research methodology

For this article, it has been assumed that the research methodology boils down to searching for facts and their meaning or implications concerning the method of designing, producing and maintaining a document called an SoA for the certification process and the effectiveness of an ISMS in an organization. The resulting product and research results constitute an authentic, verifiable contribution to knowledge in the field of information security engineering.

The research presented in this article is descriptive and comparative. This determines the lack of a research hypothesis. The research aims to accurately present the features, properties, types, advantages and disadvantages of SoA schemes currently available on the market in information security and then develop a proprietary solution. Comparative research deals with the general problem of focusing on SoA document design and generation methods as techniques and tools, not on methodologies as justification logic. A researcher needs a lot of data to conduct comparative studies – tools or collection techniques. Tools can vary in complexity, interpretation, design, and administration. Each tool is suitable for gathering a specific type of information.

Select from the available tools those that will provide the data you are looking for to test your hypothesis. It may happen that the existing research tools are not suitable for this purpose in certain situations, so the researcher should modify them or construct their own.

The primary research process led to developing an SoA model – a schema – and then constructing a methodology for its development and generation in paper and/or electronic form. The methodology takes into account such groups of areas (set of columns) in the structure of the table and their attributes, which, according to the members of the problem/research team, allow for a relatively objective and accurate assessment of the quality and/or usefulness of the SoA. Because individual rows in this table may have different values concerning the columns distinguished in the SoA, it is necessary to indicate or assign an appropriate set of techniques and tools enabling the introduction of these data.

Research findings

SoA model concept. The literature analysis on the subject shows that there is no single template [structure/layout or construction] of an SoA document (Goel & Nussbaum, 2021; Miller & Murphy, 2009). Such a situation does not make it easier to understand what an SoA is, and even more so what is meant by its scheme/structure. In the literature on the subject and found on the Internet, you can find many schemes or structures of an SoA document and tools supporting their creation, maintenance and improvement. Software solutions (Goel & Nussbaum, 2021; Walkowski et al., 2019) supporting the process of defining the structure, layout, or scheme of an SoA document and the process of its generation in the form of various solutions/reports can be divided into two groups (www.itgovernance.co.uk, advisera.com):

- Comprehensive solutions or platforms,
- Dedicated toolkits.

In terms of systems theory, the SoA document can be written symbolically as a generalized Cartesian product:

$$f\colon I \to \bigcup_{i\in I} K_i \text{ or } DS \subseteq \prod_{i\in I} K_i$$

where: $\{K_i\colon i \in I\}$ - a set family reflecting the features or properties (hereinafter also referred to as attributes) of the SoA.

Each highlighted attribute describes its mandatory or optional element. Using the formal approach, we can assume that an SoA is a relational model based on the mathematical concept of relations. In short, the n-segment relation (n-narn) is any subset of the Cartesian product of certain sets:

$$\text{SoA} \subseteq K_1 \times K_2 \times \cdots \times K_n$$

In the formal scheme/layout approach, SoA we call a non-empty set of attribute names (attributes in short) $\text{SoA} = \{A_1, A_2 \cdots, A_n\}$. Each attribute A_i is assigned a set of values Dom (A) called the domain (domain, data type, set of values) of the attribute A. It is a named and finite set of values that a given attribute can have. Schema Instance DS is the relation on the set of A_i attribute domains:

$$DS \subseteq Dom(A_1) \times Dom(A_2) \times \cdots \times Dom(A_1)$$

Since each SoA document is inherently related to its SoA relationship schema, it is often possible to find multiple SoA assigned to the same schema. So an SoA is nothing more than a finite set of k tuples with a specific scheme. Consequently, in the relational model, and therefore in the SoA, tuples cannot be repeated. Later in this final paper, the concept of a tuple will be equated with that of a control or SoA control.

The minimum number of domains in SoA is determined by the principle of the need to include the so-called mandatory controls that enable (Fig. 3):

- Identification of which controls (safety measures) will be applied, including recommended or suggested controls from ISO 27001 Annex A and potentially controls from other sources,
- justification for including the applicable controls,
- Determining the implementation status of the applicable controls (i.e. whether they are being implemented or not),
- justification for excluding controls from Annex A, which are not applicable.

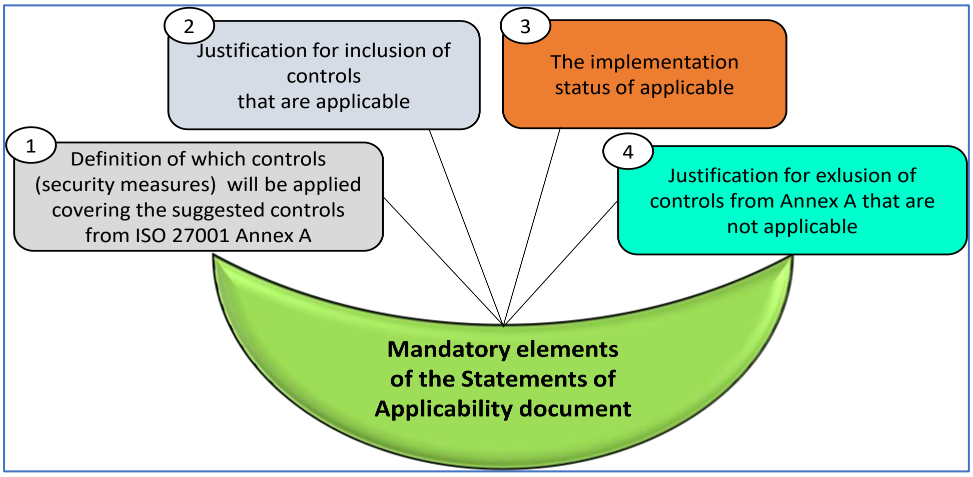

2
Justification for inclusion of controls that are applicable
3
The implementation status of applicable
1
Definition of which controls (security measures) will be applied covering the suggested controls from ISO 27001 Annex A
4
Justification for exlusion of controls from Annex A that are not applicable
Mandatory elements of the Statements of Applicability document

Fig. 3. The minimum number of domains in SoA
Source: Own study

Schematic illustrations of such SoA solutions are shown in Figure 4.

A.17 Information security aspects of business continuity management
A.18 Compliance

ISO 27001 Clause	Control	ISO/IEC 27001:2013 Control	Document
A.7.3	Termination and change of employment		
A.7.3.1	Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	• IS Security Policy
A.8	Asset management		
A.8.1	Responsibility for assets		
A.8.1.1	Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	• Asset Management Policy
A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	• Asset Management Policy
A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	• Asset Management Policy
[illegible]	[illegible]	All employees and external party users shall return all of the organizational assets in their possession upon termination [illegible]	[illegible]

Fig. 4. Illustration of exemplary SoA documents from the point of view of their mandatory elements – example
Source: own elaboration

As shown in the figure above, the number of highlighted elements – (table columns) – in the SoA structure is not very numerous.

As a proprietary solution, we propose the following SoA model:

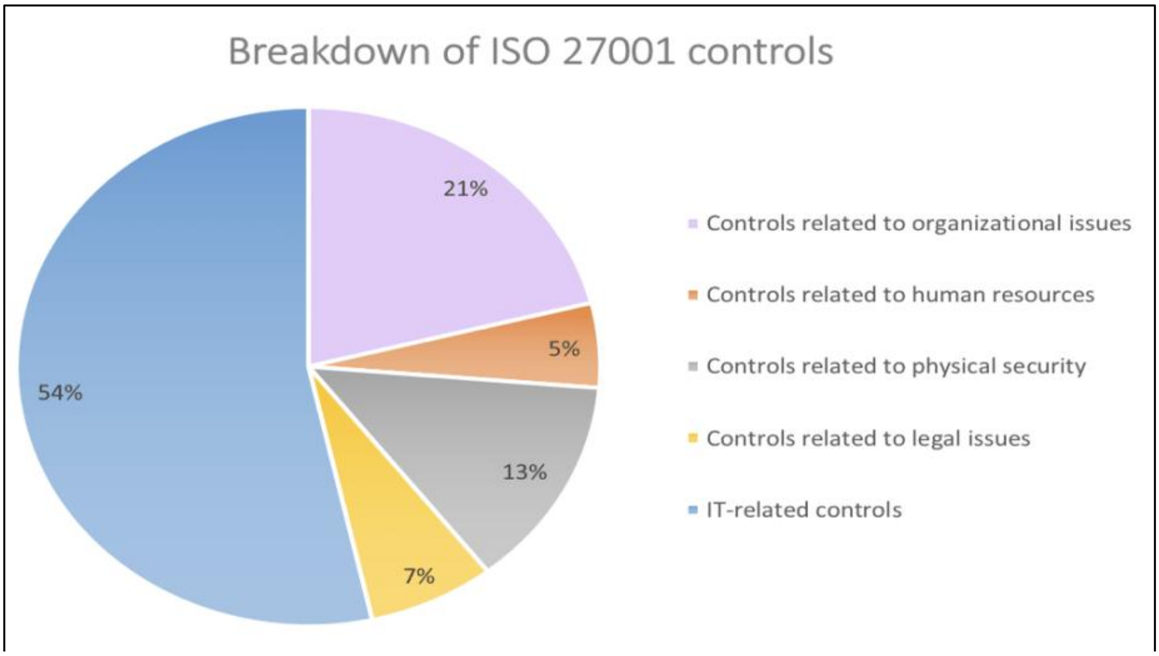
$$SoA \subseteq \mathbb{S} \times \mathbb{E}\ \times \mathbb{Z} \times \mathbb{U} \times \mathbb{W} \times \mathbb{P} \times \mathbb{D} \times \mathbb{M} \times \mathbb{F}$$

where:
$\mathbb{S}$ – a set of section names per Annex A of ISO 27001,
$\mathbb{E}$ – a set of control or control element names,
$\mathbb{Z}$ — a set of indicators reflecting the application/implementation status in the ISMS,
$\mathbb{U}$ — a set of justifications/objectives for the inclusion of controls that apply,
$\mathbb{W}$ — a set of justifications/objectives for excluding controls,
$\mathbb{P}$ — a set of reasons for selecting or applying security/control,
$\mathbb{D}$ — a set of implementation methods, evidence or comments and details about the control
$\mathbb{M}$ — a set of monitoring methods,
$\mathbb{F}$ — set of indicators reflecting the frequency of monitoring.
The set of section names can be decomposed as follows:

$$\mathbb{S} = \mathbb{S}^{O} \cup \mathbb{S}^{ZL} \cup \mathbb{S}^{IT} \cup \mathbb{S}^{BF} \cup \mathbb{S}^{P},$$

where:
$\mathbb{S}^{O}$ – a set of sections related to organizational issues: A.5, A.6., A.8, A.15,
$\mathbb{S}^{ZL}$ - a collection of sections on human resources: A.7,
$\mathbb{S}^{TI}$ - a set of IT-related sections: A.9, A.10, A.12, A.13. A.14, A.16, A.17
$\mathbb{S}^{BF}$ – a set of physical security sections: A.11
$\mathbb{S}^{P}$ – a set of legal sections: A.18.

The percentage breakdown is as follows:



Looking at the chart above, we can see that over 50% are control points related to your IT infrastructure. This is why cybersecurity specialists strongly rely on the ISO 27001 standard.

Author's proposal of the Statement of Applicability – example. This document aims to define which controls are appropriate to be implemented in the organization, the objectives of these controls, and how they are implemented and approve residual risks and formally approve the implementation of the controls. This document includes all controls listed in Annex A of the ISO 27001 standard. Controls apply to the entire Information Security Management System (ISMS) scope. Users of this document are all employees of an organization who have a role in the ISMS. The first version of the statement applicability will need updating more frequently.

To begin with, during the implementation of ISO 27001 and the new ISMS, the document will need monthly updates until the new systems have all been implemented. A well-prepared Declaration is an excellent audit guide during certification audits! To correctly fill in the SoA template:

- Complete the list of legal, regulatory and other requirements and the risk treatment table – these two documents are the primary input to writing an SoA.
- Based on the data of these two input documents, a decision has to be made as to whether the control is applicable or not, i.e. whether it is needed to meet the requirement or to reduce the risk (Dubois et al., 2010).
- If the control is applicable, it is enough to find the document related to this control, e.g. in the 'List of documents', and specify its name. The SoA template can contain default documents for most of the controls.

A schematic illustration of a fragment of a completed SoA document per the original concept of the solution is presented in the table below:

Creating an SoA demonstrates that the organization has considered a comprehensive set of candidate controls and that the applicability (or otherwise) of each has been duly considered per the requirements of ISO 27001 (see: ISO/IEC 27001:2013; ISO Standard 27001 and ISO Standard 27002). The SoA specifically justifies the inclusion or exclusion of candidate controls (whether sourced from ISO 27001 Annex A, from the ISM, or other sources) as appropriate for your environment and business delivery model. Controls may also be identified and added to the SoA required for other reasons. For example, because of legal or regulatory requirements, specific contractual requirements, or strategic or marketing purposes.

Table 3. A fragment of the SoA from the point of view of the author's solution

Requirements PN-ISO / IEC 27001: 2014 Annex A	Control applied	Selected security features and reasons for using security features	Implementation methods (including related documents, procedures and instructions)	frequency of monitoring

	Model list of security and security targets Type of security	Implemented	Planned implementation	Out of the question	Business requirements	Legal Requirements	Good practices	Risk analysis results		
𝕊	𝔼	ℤ		𝕎	𝕌/ℙ				𝔻	𝕄/𝔽
A.5 Information security policies A.5.1 Information security policies determined by management Purpose: To provide guidance and support by management for information security activities per business requirements and relevant legal standards and regulations.										
A.5.1.1 Policies for information security	**Organizational security:** A set of information security policies should be defined, approved by management, published and communicated to employees and relevant external parties.	X			X	X			The Integrated Management System Policy, the Information Security Policy in the Organization and the Statement of Applicability of the requirements of the PN-ISO / IEC 27001: 20014 standard have been approved by the management and published on the intranet for the attention of all employees. Thus, these documents were communicated to the relevant external parties. The Information Security Policy is supported by thematic policies, standards and principles. All policies referred to in other controls of this Statement of Applicability.	Verification during internal audits of individual processes. / At each internal audit
		Justification of the choice of collateral: Informing employees and other interested parties about information security objectives and commitment to meeting applicable information security requirements in the company and continuous improvement in this area.			**Fulfillment:** Management Policy issued as an attachment to the White Book approved and communicated to employees by placing on the board and the intranet site.					
A.5.1.2 Review of information security policies.	**Safeguard:** Information security policies will be reviewed at scheduled intervals or in the event of significant changes to ensure their continued suitability, adequacy and effectiveness.		X		X	X	X	X	Each policy has a designated owner who has to review the document at planned intervals. A business strategy, regulations, legislation, contracts, and related security objectives may be threatened by the environment and may change. This results in the need to review policies at planned intervals or any timeframe. This is best practice and reduces information security events in a fast-evolving world. .	Verification of the validity of the Policies during the Management review / Once a year.
		Justification of the choice of collateral: Maintaining the relevance and adequacy of the IMS Policy, ISMS Policy and other system documents.			**Fulfillment:** The suitability assessment is one of the inputs to the management review.					

Source: own elaboration

Conclusions

The organization implementing the Information Security Management System (ISMS) following the requirements of the ISO 27001 standard must analyze each of the sub-items of Annex A and refer them to its own threats and security measures. It is helpful to have a very good SoA in this process. A well-presented and easy-to-understand diagram of the SoA document shows the relationship between the applicable and implemented controls set out in Annex A, taking into account the risks and information assets of the entire organization. This gives the auditor or other stakeholders great confidence that the organization takes information security management seriously, especially when combined into an overall information security management system. The primary conclusions are:

1. There are no exact rules for developing your SoA as ISO 27001 recognizes that details of cyber security are unique to your business requirements. However, you must include:
   - An explanation of the elements of the security controls you've chosen to mitigate risks, and a justification for why you've included them. These are decided through performing a gap analysis and risk assessment in the starting stages of your ISO/IEC 27001 implementation.
   - If you have excluded any part of ISO/IEC 27001's Annex A, a list of 114 control objectives and explanations of what they are, what they do, and why.
2. The statement of applicability is part of the risk assessment and Information Security Management System (ISMS) component of ISO/IEC 27001. It is a framework of policies surrounding your cyber security systems' legality, physicality, and technicality.
3. Completing the statement of applicability (SoA) is a requirement of the ISO/IEC: a document you must develop, prepare and submit as part of your steps toward best practice regarding your data management systems.
4. The SoA is the roadmap to the efficient and effective implementation and operation of ISO 27001. It is a comprehensive document that identifies and categorizes the elements of information security measures by product and department and many other criteria.
5. In ISO 27001 certifications, the SoA document is critical as it provides physical evidence to the auditor that the necessary steps have been taken to obtain ISO 27001 certification.
6. After considering the diagrams, tables, types, advantages and disadvantages of several SoA solutions under study, it was found that the suitability and/or specificity of each solution depends on general goals, resulting, for example, from the principles of good practice and information security engineering or an individual SoA goal, such as outlined by the authors of this study.

References

Al-Mayahi, Mansoor P. (2008). ISO27001 gap analysis – case study.

Chi-Chun L., Wan-Jia C. (2012). A hybrid information security risk assessment procedure considers interdependences between controls. Expert Systems with Application. 39: 247–257.

Dubois E., Heymans P., Mayer, R. Matulevicius N. (2010). A Systematic Approach to Define the Domain of Information System Security Risk Management. Intentional Perspectives on Information Systems Engineering.

Goel S., Nussbaum B., (2021). Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. IEEE Open Journal of the Communication Society. 2021, 2, 1082–1093. [CrossRef].

How to develop a Statement of Applicability according to ISO 27001:2017, March 2018, Edition 2.0. https://www.neupart.com/ [20.05.2022].

Miller H., Murphy R. (2009). Secure cyberspace: answering the call for intelligent action, IT Professional.

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements, 2013.

ISO Standard 27001 – Information security management systems – Requirements https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/ [20.05.2022].

ISO Standard 27002 – Information technology – Security techniques – Code of practice for information security controls, https://shop.bsigroup.com/ProductDetail/?pid=000000000030347481 [21.05.2022].

Payment Card Industry – Data Security Standard (PCI DSS), https://www.pcisecuritystandards.org/security_standards/index.php [21.05.2022].

SANS Institute – Twenty Critical Security Controls for Effective Cyber Defence http://www.sans.org/critical-security-controls/ [22.05.2022].

NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [22.05.2022].

The Danish Agency for Digitization (Digitaliseringsstyrelsen) ISO 27001-benchmark http://www.digst.dk/Arkitektur-og-standarder/Styring-af-informationssikkerhed-efter-ISO-27001/~/media/Files/Arkitekturogstandarder/[23.05.2022].
InformationssikkerhedefterSO27001/ISO27001_Benchmark.ashx [23.05.2022].

Walkowski M., Biskup M., Szewczyk A., Oko J., Sujecki S. (2019). Container Based Analysis Tool for Vulnerability Prioritization in Cyber Security Systems. In: Proceedings of the 2019 21st International Conference on Transparent Optical Networks (ICTON), Angers, France, 9–13 July 2019; IEEE: Piscataway, NJ, USA. [CrossRef].

Tools and Software Solutions. https://www.itgovernance.co.uk/it-governance-tools [24.05.2022].

Tools and Software Solutions. https://advisera.com/27001academy/product-tour/[24.05.2022].