Is Applying ISO Standards to Information Security the New Black in Translation?

The ISO 18587 standard offers best practices for using and processing content through machine translation. Moreover, considering that machine translation may pose a risk to the security and confidentiality of the content to be translated, we should also rely on the ISO 27000 series, which offers a framework of international standards for organizations and professional translators to manage their information assets. The application of these standards is a quality seal of a more secure and reliable service.

By Dolores R. Guiñazú and Gabriela Escarrá

Quality is not subjective. Quality has to be measured. What gets measured, gets managed."

The above quote from *The Practice of Management* by Peter Drucker[1], published in 1954, is still relevant today.

ISO standards furnish translation services providers (TSPs) and organizations with a basis for achieving the best possible quality, improving customer satisfaction, and reducing errors to a minimum. They include the industry best-practices that facilitate processes. The well-thought-out application of these processes, including monitoring and measurement, is crucial for ensuring that an organization is performing as designed and thus meeting quality requirements. As a result, TSPs can stand out and differentiate from their competitors and increase their potential for profit and customer loyalty.

Post-Editing and ISO 18587:2017

Technology is quickly evolving, and that's changing the way we used to work. Artificial intelligence (AI) is the ability of a computer program or machine to learn and perform tasks that were previously done by humans. As AI becomes increasingly sophisticated and precise, the growing demand for such services as post-editing machine translation (MT) and remote interpreting via Zoom or other online platforms continues to impact the translation and interpreting professions worldwide.

Some translators may panic and feel terrified about the possible automation of our profession. However, like many other professionals, we strongly believe that we have to embrace and leverage this new reality. For instance, in episode 49 of *The ATA Podcast*[2], Jay Marciano, director of MT outreach and strategy at Lengoo, states that we all need a positive attitude toward technological change. He emphasizes that technology is just another tool like a hammer and that we should all try to learn how to use it in the right way. In almost every area of life, technology is used as a supplemental aid to what people used to do manually. Thus, making friends with the latest available technology is an imperative of life.

In the past few years, the use of MT has been on the rise to meet the increased demand for multilingual content. Many perceive MT to be slightly cheaper and faster than human translation. However, we must be tech-savvy and

Even though the advantages of post-editing are many, the information security threats posed by some MT engines cannot be ignored.

bold when seizing this new technology to enhance the provisioning of our services. As translators, we must dare to walk new paths in our profession. Moreover, due to the variable quality of MT, it's necessary to combine MT with post-editing. In response to this need, the International Organization for Standardization (ISO) has greatly contributed to setting the requirements for post-editing through ISO 18587:2017—Translation Services—Post-Editing of Machine Translation Output—Requirements.[3]

ISO is a non-governmental organization that determines specifications for products, services, and systems for quality and efficiency. It gathers experts in a particular subject area to create a standard. The organization's abbreviated name—ISO—is not an acronym; it derives from the ancient Greek word *ísos*, meaning equal or equivalent. Because the organization would have different acronyms in different languages, the founders of the organization decided to call it by the short form ISO. It was founded in 1947, and since then it has published 23,943 international standards covering almost all aspects of technology and business.

In our current scenario, ISO 18587:2017 Translation Services—Post-Editing of Machine Translation Output—Requirements is a necessary guideline for the pre-production, production, and post-production of post-editing jobs. ISO 18587:2017 begins with a focus on the delivery of MT output, followed by human post-

editing, and its intended use by TSPs, their clients, and post-editors. The standard sets out exactly how and to what extent MT output should be revised and edited.

By following the processes recommended in this standard, TSPs can achieve a great balance between time, cost, and quality. A qualified post-editor should check the MT output for completeness and accuracy, verify the grammar, syntax, and semantics of the text, and ensure that it meets all the expectations in terms of style, formatting, and terminology.

MT Engines and Information Security

Even though the advantages of post-editing are many, the information security threats posed by some MT engines cannot be ignored. The main risk is largely dependent on the server, engine, or computer that's being used and who has access to that information.

Apart from considering the use of protected MT engines with controlled access to the content and fewer people involved, TSPs should follow strict processes to keep information assets secure, streamline workflows, manage sensitive information, and avoid any critical data leak. To that end, TSPs should have the necessary knowledge of the ISO 27000[4] family of information security standards published by ISO in partnership with the International Electrotechnical Commission (IEC). This series of standards enables organizations to manage the security of assets such

as financial information, intellectual property, employee details, or information entrusted by third parties.

The requirements set forth in this standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. What follows is an overview of the main standards found in this family. (See Figure 2 for a table of the entire ISO 27000 family and how the standards relate to one another.)

ISO/IEC 27000:2009—Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary[5]: Provides an overview of the information security management systems (ISMS) family of standards. ISO/IEC 27000:2009 also provides an introduction to ISMS and a brief description of the Plan-Do-Check-Act (PDCA) cycle. The PDCA cycle is a four-step model for carrying out change. Just as a circle has no end, the PDCA cycle should be repeated for continuous improvement. The PDCA cycle is considered a project planning tool. (See Figure 1.)

ISO/IEC 27001:2013—Information Security Management Systems[6]: Specifies the requirements for establishing, implementing, maintaining, and continuously improving an ISMS within the context of an organization.

Similar to how ISO 9001:2015—Quality Management Systems—Requirements is considered the leading international

standard for quality management systems in almost every industry, ISO/IEC 27001:2013 is the leading international standard for an ISMS. An ISMS helps organizations secure the confidentiality, integrity, and availability of information assets. An ISMS is composed of policies, procedures, and other controls entailing individuals, technology, and processes.

Organizations that are serious about data protection should have a process in place to classify their information assets according to the level of protection they should be given. Information assets should be divided into four main levels according to the degree of confidentiality:

1. Confidential: only accessible to senior managers

2. Restricted: accessible to almost every employee

3. Internal: accessible to all employees

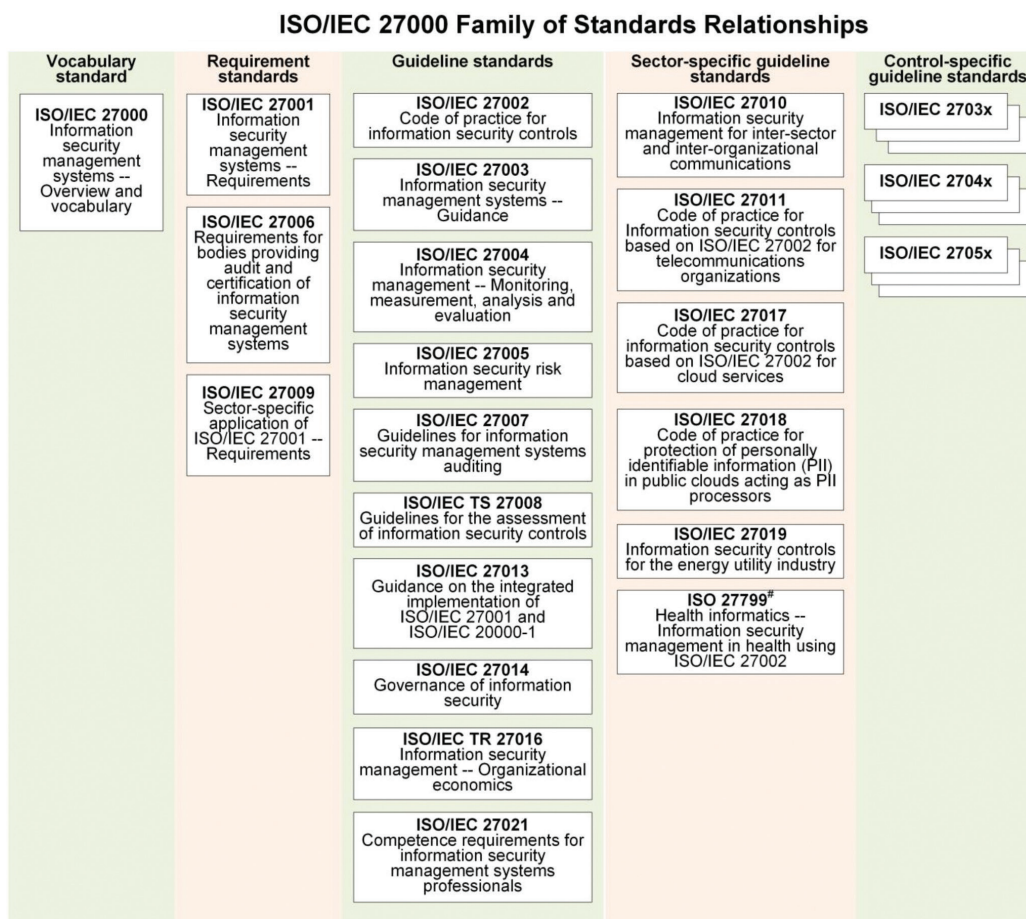4. Public Information: accessible to everyone.

In some cases, certain sublevels may be created for specific job functions.

Once the information assets involved in the translation are classified, the risks associated with them determined, and the various ways to treat them specified, the TSP or translator can ensure a secure treatment of the information contained in the source document. In addition, ISO/IEC 27001:2013 requires all risks to be assigned to an owner who is responsible for approving any risk treatment plans. (In general, the owner is the one in charge of the area, such as the marketing

Figure 1: PDCA cycle applied to ISO/IEC 27001 (Source: http://bitly.ws/g5Sc)[7]

PLAN
- Define business objectives
- Define risk assessment methodology

DO
- Manage information security risks
- Implement risk control procedures

ACT
- Conduct periodic risk assessments
- Implement correction actions
- Implement preventive actions

CHECK
- Monitor and measure
- Control non-conformity
- Identify root causes

Figure 2: The ISO/IEC 27000 Family of Standards[10]

ISO/IEC 27000 Family of Standards Relationships

Vocabulary standard	Requirement standards	Guideline standards	Sector-specific guideline standards	Control-specific guideline standards
ISO/IEC 27000 Information security management systems -- Overview and vocabulary	ISO/IEC 27001 Information security management systems -- Requirements	ISO/IEC 27002 Code of practice for information security controls	ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications	ISO/IEC 2703x
	ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems	ISO/IEC 27003 Information security management systems -- Guidance	ISO/IEC 27011 Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations	ISO/IEC 2704x
	ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 -- Requirements	ISO/IEC 27004 Information security management -- Monitoring, measurement, analysis and evaluation	ISO/IEC 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services	ISO/IEC 2705x
		ISO/IEC 27005 Information security risk management	ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	
		ISO/IEC 27007 Guidelines for information security management systems auditing	ISO/IEC 27019 Information security controls for the energy utility industry	
		ISO/IEC TS 27008 Guidelines for the assessment of information security controls	ISO 27799# Health informatics -- Information security management in health using ISO/IEC 27002	
		ISO/IEC 27013 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1		
		ISO/IEC 27014 Governance of information security		
		ISO/IEC TR 27016 Information security management -- Organizational economics		
		ISO/IEC 27021 Competence requirements for information security management systems professionals		

> Given that MT output does not equal the quality and accuracy of human translation, human post-editing is required to ensure high-quality translations while speeding up processes and shortening delivery times.

director in the commercial area or the head of human resources in that department.)

This PDCA cycle is a continuous loop of planning, doing, checking, and acting. It's just a reminder of how a simple and effective approach can help us solve problems and manage change.

ISO/IEC 27002:2013—Information Technology—Security Techniques—Code of Practice for Information Security Controls[8]: This is a supplementary standard that provides a code of practice for ISO/IEC 27001:2013 that recommends specific information security controls addressing information security control objectives arising from risks to the confidentiality, integrity, and availability of the information assets to be handled by the TSP or translator.

ISO/IEC 27007:2020—Information Security, Cybersecurity and Privacy Protection—Guidelines for Information Security Management Systems Auditing[9]: This standard is applicable to those who need to understand or conduct audits to ensure the secure handling of the information assets by the TSP or translator. This document concentrates on ISMS internal audits (first party) and ISMS audits conducted by organizations on their external providers and other external interested parties (second party).

Final Thoughts

The post-editing process is extremely dynamic with a diversity of issues to be considered. The use of MT and post-editing may involve some risk factors related to the lack of qualified post-editors and the possibility of data breaches depending on the engines that are used. These potential risks must be identified and addressed. Thus, a strong focus on ISO standards for ensuring that the best processes and practices for post-editing and information security management are followed are crucial to consolidating our professionalism, ethics, and relevance as highly competitive post-editors. ⒶⓉⒶ

NOTES

[1] Drucker, P.F. (1954), *The Practice of Management*, Harper, New York, NY.

[2] Episode 30 of The ATA Podcast with Jay Marciano can be found at *https://bit.ly/ATA-Podcast30*. Episode 49, also featuring Jay, can be heard at *https://bit.ly/ATA-Podcast49*.

[3] ISO 18587:2017, *https://bit.ly/3ry7tbX*

[4] ISO 27000 series, *https://www.27000.org/*

[5] ISO/IEC 27000:2009, *https://bit.ly/3zxffG0*

[6] ISO/IEC 27001:2013, *https://bit.ly/3y18VpD*

[7] PDCA Cycle applied to ISO/IEC 27001:2013, *https://bit.ly/3y50Wb8*

[8] ISO/IEC 27002:2013, *https://bit.ly/3i32vkm*

[9] ISO/IEC 27007:2020, *https://bit.ly/3wYi5lv*

[10] An Overview of ISO/IEC 27000 Family of Information Security Management System Standards, published by the Office of the Government Chief Information Officer Updated in May 2021, *https://bit.ly/3BvlHhr*

Dolores R. Guiñazú is a certified sworn (court-approved) translator and interpreter. She is also a copyeditor. She has an MBA in marketing management from the Universidad del Salvador and Albany University—State University of New York. She is an ISO 27001:2013 Internal Auditor and has certifications from the Translation Automation User Society in post-editing and transcreation. She works for agencies and direct clients all over the world. She is co-author of *Mejora continua de la calidad en la traducción.* She is also the host and creator of the Podcast *ATTITUDEABLE*. *dolores@liftvalue.com*

Gabriela Escarrá is a certified sworn translator. She is an ISO 27001:2013 Internal Auditor and she has certifications from the Translation Automation User Society in post-editing and transcreation. She works as a translator, editor, post-editor, and transcreator specializing in marketing and corporate communication for international agencies and direct clients. She is co-author of *Mejora continua de la calidad en la traducció*n. She has a degree in teaching English and literature from the University of La Plata. *gabriela@langtic.com*