An Overview of Information and Cyber Security Standards

Hugh Boyes* and Matthew D. Higgins

WMG, University of Warwick, Coventry, CV4 7AL, UK
E-mail: hugh.boyes.1@warwick.ac.uk; m.higgins@warwick.ac.uk
**Corresponding Author*

Received 12 July 2024; Accepted 28 August 2024

Abstract

Advances in digitalization, particularly those regarding cyber-physical systems (CPS) have stimulated the adoption of digital capabilities such as Industrial IoT, machine learning, cloud services, and the use of digital twins. The increased digital sophistication of CPS is not without risk, particularly regarding the potential for information/cyber security incidents. Whilst the need for security of enterprise information security is not new, A significant challenge is understanding what security standards may be available and applicable when developing security controls and technical measures to protect CPS. This paper explores what research is available regarding the choice and comparison of information/cyber security standards. It provides a snapshot of the security standards landscape at the start of 2024. Issues relating to development and adoption of security standards are examined, illustrated using inconsistencies in language regarding three key terms: availability, integrity, and confidentiality.

Keywords: Information security, cyber security, standards, security goals, security domain.

Journal of ICT Standardization, Vol. 12_1, 95–134.
doi: 10.13052/jicts2245-800X.1215

1 Introduction

Across all industrial sectors cyber-physical systems (CPS) are being designed or upgraded by incorporating greater digital processing to achieve goals e.g., enhanced performance, improved visualization, or to enable integration with other CPS and enterprise systems. While this increased digitalization enables new opportunities and insights, it also significantly increases the exposure of these systems to outside influences and interference. In parallel with this increased exposure rapid increases are observed in cyber criminals' capability to detect and exploit system vulnerabilities. Typically, such activity has mainly focused on enterprise systems targeted for theft of information or denial of service through ransomware deployment.

Through their nature CPS offer another avenue for cyber criminals to exploit, the potential for manipulation that causes physical impact in the real world. Such malicious interference could result in damage to or destruction of the CPS, pollution or damage to the environment, and potentially serious injury or death of stakeholders. An example of real-world manipulation occurred in 2013 when organized crime accessed Antwerp port's systems to locate and exfiltrate smuggled drugs [1, 2]. Furthermore, insecure CPS provide a vector potentially enabling competitors to gain remote access to sensitive industrial intellectual property and thus understand how to gain competitive advantage.

To counter these threats, the designers, suppliers and operators of CPS need to improve the system security. Ideally such improvements would be guided by good practice as documented in national or international standards. However, a perennial problem for those developing, owning, and operating complex CPS is determining which, if any, security standards may be applicable or should be applied. In the UK, for example, certification to standards such as PCI-DSS, Cyber Essentials Plus or ISO 27001 are often mentioned. Pang et al. [3] suggest that implementing ISO 27001 could ensure the safety of the information in CPS and digital twins.

Some security professionals may question whether such standards are appropriate for CPS, e.g., for industrial and process control systems, national infrastructure, robotics and connected and autonomous vehicles. To the best of the authors' knowledge, no published work appears to inform the choice, or assess appropriateness, of available IT/cyber security standards.

Our research objective was to establish what security standards and frameworks are available and the consistency of language regarding three

key security concepts. To fulfil this objective, our research sought to answer the following questions:

- RQ1 – What existing research has been published concerning the comparison of IT security standards?
- RQ2 – What is the landscape of IT security standards?
- RQ3 – Is there a consistent use of language across the IT security standards?

Our knowledge contribution is a review of existing work regarding the comparison and analysis of IT/cyber security standards, their coverage, and their potential applicability to CPS. We identify and categorize 561 documents issued by four standards bodies and consider whether proliferation of available security standards makes the selection of relevant standards a potentially time consuming and costly exercise.

2 Scoping Study and Developing Research Methodology

2.1 Scoping the Study

During preliminary work scoping this study we identified some relevant recently published papers and sought to repeat some of their searches with mixed results. For example, an IoT-related paper [4] considered the standardization state-of-the-art regarding IoT-based smart environments security concerns. The authors used the search string {"Security Standard" OR "Security Assessment Framework" OR "Security Techniques"} [4] in five identified databases. They reported that these searches yielded the volumes of papers listed in Table 1. We repeated these searches and included our results in the table. It is unclear why there is such a large disparity in the volume of resources identified.

Table 1 Comparison of search results Karie et al. vs Authors' repeat of searches

Article Source	Karie et al.	Our Results	Notes
IEEExplore	38	1,085	
Google Scholar	74	17,600	
Science Direct	42	4,482	Review & Research Articles
SpringerLink	8	57,290	Articles only
Web of Science	20	1,406	
Total	182	81,863	

A comparison of security standards for SCADA systems acknowledged the volume of existing security standards and establish selection criteria for including SCADA-related standards [5]. The authors refer to conducting a comprehensive search focusing on standardization bodies and governmental agencies. Identifying eight 'standards', of US or UK origin, they provide no indication whether other nations (e.g., Germany, Sweden, Norway, Australia, etc.) or international bodies (e.g., IEC and ISO) were included in their search. While in addition to those in [5], Zhou et al. [6] identified a further five SCADA-related standards, one US, three Chinese and one Japanese, although their search methodology was no clearer.

A survey of cybersecurity standards for nuclear instrumentation and control systems [7] was mainly based on author's previous knowledge of the domain, as well as exploring some publishers' databases (e.g., IEC/ISO databases) and other cybersecurity surveys. This approach is not replicable, but the paper does identify numerous security standards, some generic and others focused on nuclear systems.

Some existing works pre-selected the standards to be compared. For example, a comparison of COBIT and ISO 27001 [8]. Preselection was considered inappropriate for this study.

A further consideration was the selection of sources of 'standards' to be regarded as in scope. There are a diverse range of standards development organizations (SDOs) issuing security-related standards. As noted by Glavič [9], relevant SDOs include official international, regional, or national standards organizations. There are also professional and industry organizations developing security standards, including Information Systems Audit and Control Association (ISACA), Information Systems Security Association (ISSA), Information Security Forum (ISF), Payment Card Industry (PCI) Security Standards Council and the Industrial Internet Consortium (IIC). For consistency we limited our study to standards published by ISO/IEC, the British Standards Institution (BSI) and the US National Institution of Standards (NIST). These represent international and national standardization organizations, with clear protocols regarding the creation and publication of standards. Experience from this limited review of existing work informed our literature search strategy which is described below.

2.2 Research Methodology

To address our research questions, we adopted a phased approach. The initial phase focused on the first research question, seeking to obtain an overview of

relevant existing literature that reviewed and/or compared security standards. The next phase focused on identifying security standards and frameworks, published by ISO/IEC, BSI and NIST. The final phase explored the linguistic consistency of three key security terms: availability, integrity, and confidentiality.

In planning the first phase, we noted the challenges documented by Karie et al. [4] regarding the high volume of material returned in their searches, with thousands or tens of thousands of hits recorded on some searches. We adopted a two-stage process for the literature search – to generate an initial corpus of material and then to extend the searches using a snowballing approach based on this corpus. As our objective was focused on the comparison and choice of security standards, we limited our initial search to those papers where relevant keywords appeared in the document title. Four searches were conducted using Google Scholar with the aim of identifying papers. the results of these searches are shown in Table 2.

Table 2 Results from Authors' literature

Search Term	Raw Results	Relevant Papers
allintitle: comparison security standards	16	9
allintitle: review security standards	54	21
allintitle: review security framework	66	2
allintitle: comparison security framework	15	2
Total	151	34

Excluding citations and books, these searches yielded a total of 151 papers. These were reviewed to assess their relevance, excluding papers that were:

- not related or relevant to comparison of security standards or frameworks,
- not addressing security of organizations or technology-based systems, e.g., those focusing on international security or financial securities,
- narrowly focused, e.g., wireless network security, web applications, credit card security (i.e., PCI DSS), etc.,
- written in a language other than English or where the full text was inaccessible.

After deduplication, this review and filtering yielded 34 papers which were subjected to detailed examination. During this review the snowballing approach identified additional relevant material, with a further 35 papers and reports added to the corpus. In total we examined 69 documents that reviewed

and/or compared security standards. Our findings from this literature review are discussed in Section 3.

The second phase focused on identification and review of IT-related security standards. While this was primarily focused on those available from four standards bodies, we also considered the industrial standards landscape. Much of the initial work for this phase drew upon standards identified and discussed in the literature review corpus. Searches were also conducted to identify relevant work by industry consortia and professional bodies. An important consideration in this analysis, was the security of what, for whom and in respect of what risks.

The final phase, discussed in Section 5 considers the linguistic challenge identified by Robinson [10]. It focuses on three key security concepts (availability, confidentiality, and integrity) that underpin much of the IT/cyber security literature. We discuss our findings in Section 6 and set out our conclusions in Section 7.

3 Review of Existing Work

3.1 Coverage of Standards by Existing Work

Reviewing the corpus of 69 papers we sought to identify the most cited standards, the results are shown in Table 3.

Table 3 Coverage of standards by existing work

Standard or Series	Citations	Focus
ISO 27001/2	44	Organization (ISMS)
Common Criteria (ISO 15408 series)	20	Security Evaluation
COBIT	20	Organization (ISMS)
ISO 27005	14	Risk
IEC/ISA 62443 series	14	Industrial systems
NIST SP 800-53	14	Organization (ISMS)
ISO 17799	12	Organization (ISMS)
ITIL (ISO 20000 series)	10	Organization (ISMS)
NIST SP 800-30	8	Risk
NIST SP 800-82	8	Withdrawn
GASSP/GAISP	7	Organization (ISMS)
ISO 27019	5	Organization (ISMS)
NIST SP 800-39	5	Organization (ISMS)
ISO 13335	3	Withdrawn

This is a relatively narrow set of standards when compared to the totality of IT/cyber security-related standards identified in Section 4. We can divide the above list into four categories comprising those:

- standards aimed at developing information security management systems or practices at an organization level (i.e., ISO 27001/2, ISO 27005, NIST SP 800-30, NIST SP 800-53, COBIT, GASSP/GAISP, ITIL (ISO 20000) and ISO 27019 (Note - the latter focusses on the energy utility industry),
- standards related to the security evaluation of IT systems, i.e., Common Criteria (ISO 15408 series),
- standards related to the security of industrial automation and control systems, i.e., IEC/ISA 62443 series and NIST SP 800-82, and
- standards that have been withdrawn or superseded, i.e., ISO 17799 and the ISO 13335 series.

The research coverage is dominated by those standards focusing on organizational information or cyber security and the creation of organization wide policies and practices to manage information/cyber security through information security management systems (ISMS).

3.2 Review of Existing Work

In reviewing the corpus of selected papers, an emergent issue was whether an included standard was current, i.e., neither withdrawn nor superseded. For example, ISO/IEC 17799:2000 [11], was published in December 2000 and withdrawn on the publication of ISO/IEC 27002:2005 [12]. ISO 17799 is referenced by twelve of the reviewed papers, of which only two were published prior to its withdrawal [13, 14]. Such citations are only relevant to tracing evolution of standards (e.g., BS 7799 into ISO 17799 then into ISO/IEC 27002), or examination of prior work. Superseded standards are irrelevant when considering the current standards portfolio.

Frangopoulos and Eloff [13] undertook comparative study of four standards ISO 17799, BS 7799-2, Common Criteria (ISO 15408), Computer Emergency Response Team (CERT) Practices and GASSP/GAISP. Their comparison of ISO 15408 to ISO 17799, suggests a misconception regarding the purpose of these two standards. The former supports evaluation or assurance of IT systems, whereas the latter was intended to cover an entire organization, or at least a significant self-contained portion of it.

Examination of CERT Practices and GASSP/GAISP demonstrated numerous coverage gaps in comparison to ISO 17799 [11]. This outcome was

perhaps inevitable as the three documents approach security from different perspectives and with different objectives. Similar findings were reported by Evans et al. [14] in a comparison of ISO 17799 to three standards aimed at securing industrial control system.

Some papers provided a thematic review of standards related to a technology field or business area, e.g., Trappey et al. [15] identify standards and patents relevant to IoT, while Leszczyna [16] focuses on standards relevant to cyber security of smart electricity grids. In contrast to Trappey et al. [15], Karie et al. [4] identified some 80 ISO/IEC security standards, 32 ETSI standards and 37 different security frameworks including 7 NIST special publications on security techniques. Their research essentially catalogues standards they consider relevant to IoT. Whilst informative this illustrates the challenge faced by those seeking to secure CPS, i.e., how to identify relevant standards.

An interesting aspect of Leszczyna's research [16] is the exploration of relationships between requirements in the identified standards. This illustrated how some standards act as inputs to development of other standards, congruence between some standards, and use of horizontal lanes to depict scope and the generality and/or thematic coverage of standards [16]. This approach will be considered further in Section 4.

A conceptual approach proposed by Tsohou et al. [17] comprises a four-layer classification framework employed to categorize information security standards. These layers and associated ISO standards address: security requirements (ISO 27001); security risks (ISO 27005); security controls (ISO 27002); and the implementation of safeguards (e.g., intrusion detection (ISO 18043), or network security management (ISO 18028 series)). Their approach has limitations, e.g., the poor coverage of the "Act" phase of the PDCA-cycle which is inherent in ISO 27001. By grounding the approach using ISO 27001 it suffers the weaknesses inherent in that standard.

In contrast to Tsohou et al. [17], Beckers et al. [18] developed a conceptual model for structured comparison of security standards, drawing on work concerning healthcare telematics security (HatSec) [19]. Beckers et al. [18] define a common terminology, based on ISO 27001 augmented with relevant terms from other studies. Table 4 compares the analysis steps proposed by Beckers et al. [18] and Sunyaev [19]. The overall approach adopted by Beckers et al. [18] seeks to provide information to populate a security standards template, which has merit in terms of populating a catalogue of standards. However, it does not address what combination of standards may be required to cover both the overall security requirements and any detailed requirements

Table 4 Comparison of Analysis Steps [18]

HatSec Phases	HatSec Analysis Steps	Modified Analysis Steps
Security Analysis Context and Preparation	Scope Identification	Environment Description
		Stakeholder Description
	Asset Identification	Asset Identification
		Risk Level Definition
Security Analysis Process	Basic Security Check	Security Property Description
	Threat Identification	Control Assessment
	Vulnerability Identification	Vulnerability & Threat Analysis
		Risk Determination
Security Analysis Product	Security Assessment	Security Assessment
	Security Measures	Security Measures
		Risk Acceptance
		Security & Risk Documentation

associated with a specific system or systems architecture (i.e., the Level 4 analysis by Tsohou et al. [17]).

Papers concerning categorization and comparison of security standards for cloud computing [20, 21] are over reliant on ISO 27001-based security management. Of the nineteen security aspects identified by Paudel et al. [20], eleven aspects were not addressed by ISO 27001 and nine were not addressed by ISO 27002. Whereas Di Giulio et al. [21] used a mapping based on the Cloud Security Alliance's (CSA) Treacherous Threats [22] and suggest that only two of the twelve threats are not covered by ISO 27001. In their analysis Di Giulio et al. [21] considered insider threats to be the most important class of threats due to omissions in the three standards. This is an interesting observation as a fundamental issue with an ISMS based on ISO 27001 is the scope covered when certifying an organization. As most cloud services and applications are hosted by third parties, this calls into question the applicability of ISO 27001 to such multi-organization situations.

de Franco Rosa et al. [23] employed a set of assessment heuristics comprising eleven security properties and six assessment dimensions. These were intended for use in selection and/or prioritization of assessment items identified in security standards. Their approach was based on a security assessment ontology (SecAOnto) [24], the relevance and validity of which depends on a user's acceptance of its security properties and dimensions. Some properties are well recognized (e.g., availability, integrity, confidentiality, authenticity, resilience, and non-repudiation), whereas the need for

others (e.g., traceability, privacy, auditability, legality, non-retroactivity) may be questionable or inappropriate for a given assessment situation.

While much of the reviewed corpus was relatively abstract in its approach, there were a few exceptions. Evans et al. [14] undertook a comparison of cross-sector cyber security standards based on Common Criteria for assessing systems and devices. This more rigorous technical approach was relevant as the authors could compare standards coverage to a published system protection profile [25].

Some reviewed papers were largely narrative in nature, e.g., describing development and evolution of standards for industrial control systems [26] or selected security standards in the ISO portfolio [27]. Whilst providing a contemporaneous view of the standards landscape, these papers are of limited utility in considering coverage, overlaps and relationship between standards.

Several works investigated mapping the security standards landscape and its coverage. For example, Mussmann et al. [28] reviewed the standards mapping procedures used in twenty-two papers, of which nineteen based their mapping strategy on security ontologies. Such comparison is subjective as few, if any, of these ontologies are rooted in a validated top-level ontology and many security-related concepts are open to interpretation. Two papers employed natural language processing (NLP) techniques to partially automate comparison of standards. Although a potentially fruitful area for future research, it is heavily reliant on correct training regarding association of terms and concepts. In support of such work there is also a need to address dissonance in the assumed security body of knowledge.

The sourcing and provenance of security ontologies for standards analysis and to support NLP training is potentially problematic. Milicevic and Goeken [29] applied an ontological approach to develop a metamodel for ISO 27001 by generating and refining a set of in-vivo codes. This methodology inherently introduces bias, for example the meaning and approach to risk. ISO 27000 [30] defines risk as *effect of uncertainty on objectives* where consequence may be positive (i.e., representing an opportunity) or negative (i.e., what is colloquially referred to as a threat). While a threat is defined in ISO 27000 [30] as a *potential cause of an unwanted incident, which can result in harm to a system or organization*. Because of assumptions inherent in the drafting of ISO 27001, only negative aspects are considered in the resulting metamodel in Figure 1. This metamodel precludes threats arising from the inadvertent action or inaction by an insider.

Sommestad et al. [5] compared eight documents related to security of SCADA and industrial automation and control systems. While they refer to

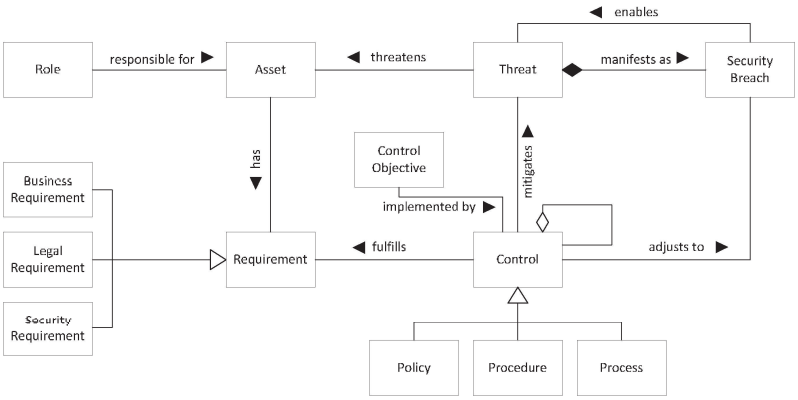

Figure 1 ISO 27001 Metamodel [29].

the documents as being standards, this is a moot point. Arguably only two sets are standards (i.e., ANSI/ISA–99.00.01–2007 Part 1-3 and NERC CIP-002-1 – CIP-009-1), the remainder are guidance issued by UK and US government organizations. Despite comparing the documents to ISO/IEC 17799, which was withdrawn in 2005 and replaced by ISO 27002 [12], their findings are valid. They concluded that the documents were focused on technical rather than operational countermeasures as specified in ISO/IEC 17799.

Ehrlich et al. [31] surveyed the industrial security standardization landscape in the context of Industry 4.0. They considered four sets of standards, noting their difference in purpose [31]:

- IEC 62443 – industrial communication networks, and network and system security
- ISO/IEC 27000 – Information technology and information security management system (ISMS)
- ISO/IEC 15408 – Evaluation criteria for IT security
- VDI/VDE 2182 – Risk-based selection of controls and countermeasures

They considered that the current approach to security is not dynamic, lacks flexibility and does not address the whole life cycle of industrial systems [31]. These are legitimate concerns given the volume and nature of current cyber security incidents.

Haufe et al. [32] undertook a process mapping study regarding ISO 27001 [33], ITIL (ISO 20000) and COBIT, identifying a total of twenty-eight processes. In respect of ISO 27001, only 16 of the processes are fully addressed, 4 are partially addressed and 8 are not addressed [32]. They

considered that three key processes not addressed in ISO 27001 were problem management, configuration management, and change management [ibid.]. Of the missing processes the lack of attention to configuration and change management are serious weaknesses given the need to manage vulnerabilities (e.g., through patching and timely changes to system configuration).

In a review of the adoption of ISMS, principally those based on the ISO 27000 series of standards, Barlette and Fomin [34] explored barriers to adoption and limitations of the standards. They discussed five limitations [34] all of which are of relevance to this research. These limitations can be summarized as follows:

- The generality of standards and their relatively static nature does not accommodate the security or business needs and operating environment of differing organizations.
- The complexity of implementing standards arising from their abstract nature, lack of guidance on interpretation of requirements, and the relative brevity with which topics/controls are generally discussed.
- A focus on checklists and observable events, while failing to address the human factor and social/societal nature of potential underlying or causal issues.
- Failure to cater for organizations of varying size and complexity, for example, the difference between an international corporation and a small or micro enterprise.

In a review of cyber security frameworks and information security standards, Taherdoost [35] citing Arora [8] suggests standards are generally classified into two main categories: information security standards and information security governance standards. This appears to misrepresent Arora's work, which considered security standards to include ISO/IEC 17799 and series such as ISO 27000 and NIST SP 800, while IT governance/service quality standards included COBIT and ITIL. Arora considered those primarily concerned with information security governance fail to adequately address how security measures integrate into information systems management and processes [8]. This observation is borne out in the various comparisons discussed earlier in this section.

3.3 Summary

Our review of existing work reveals a lack of consensus regarding what comprises a security standard, and the difference between technical standards and management standards. Existing work typically focuses on relatively

narrow subsets of standards, with the ISO 27000 series standards, particularly ISO 27001, receiving the most attention. Comparisons of existing standards largely focused on organization information security, i.e., those associated with information security management systems (ISMS) and information systems governance (e.g., COBIT and ITIL). Thus existing work does not offer a holistic solution with regards to choosing security standards or frameworks for digital twins.

4 Investigation and Analysis of Security Standards

As noted in Section 2, our search was limited to standards issued by ISO, IEC, BSI and NIST. the first three SDOs have a common approach to numbering and classifying standards, which enabled identification of standards issued by combinations of these SDOs. Our approach to searching their catalogues for relevant standards is described in Section 4.1. NIST operates its own standards and publications numbering scheme, our search is described in Section 4.2. Section 4.3 briefly discusses the limited relevant standardization activity in industry and in Section 4.4 summarize our findings.

4.1 Assessing the International Security Standards Landscape

The international classification system for standards (ICS) [36] provides a common structured approach for cataloguing and classifying standards. Our research concerns the information technology category (35) and within it the sub-category (030) concerning IT security standards. ICS is relevant to the ISO, IEC, and BSI catalogues.

Using its advanced search tool, BSI's online catalogue [37] was searched by selecting ICS category "35.030", limiting results to those with a "Current" status. ISO's catalogue [38] was searched by ICS. limiting results to those with a status "Published". Searching IEC's webstore [39] limited results to "Active" publications. These searches returned 369, 262 and 223 results respectively. Following consolidation, review and deduplication, a portfolio of 361 IT security-related standards was created. Following a detailed review, some documents was removed, including IEC Guide 120 [40], draft standards (DPCs), tracked changes versions (TC), and bundled sets of standards.

Portfolio analysis established publication dates of latest versions, see Figure 2, which is indicative of standards development activity, i.e. issue of new standards and revision or reissue of existing standards, rather than when standards were first published, i.e., growth of the standards catalogue. The

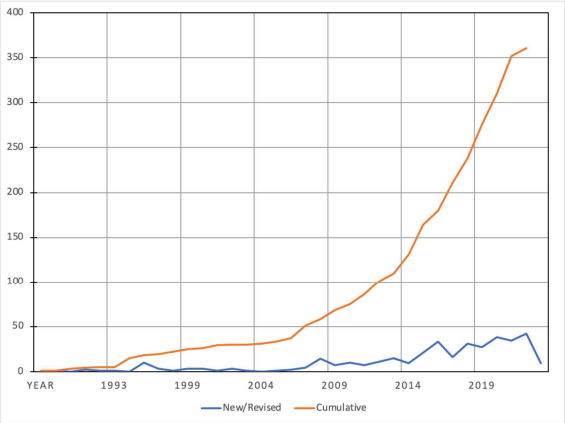

Figure 2 Number of new or revised IT security standards per annum.

analysis shows an increase in the rate of standard publication activity. For example, in 2022, 42 new, revised or amended standards were published, i.e., over 10% of the current IT security standards.

The portfolio was categorized by the main topic covered, by individual standards. Table 5 illustrates the breadth of topics covered by IT security standards, ranging from management systems and processes to detailed aspects of security related to cryptography and specific information exchange protocols. For those specifying, developing or operating CPS it is a significant challenge to know which are relevant, complimentary, or possibly even contradictory. To the best of our knowledge there are no tools that would enable a CPS developer or operator to identify relevant standards. There is a significant cost to procuring access to all these standards and given the recent rates of standards publication, there is an economic overhead for businesses seeking to maintain awareness of the current portfolio.

4.2 Assessing the NIST Security Standards Landscape

The Computer Security Resource Center (CSRC), part of NIST's Information Technology Laboratory, publishes two series of documents of relevance, the Special Publication (SP) 800 series and the 1800 series. The former comprises guidelines, recommendations, technical specifications, and annual reports of NIST's cybersecurity activities [41]. The latter presents practical, usable, cybersecurity solutions to the cybersecurity community, demonstrating how to apply standards-based approaches and best practices [42].

Table 5 IT security-related standards categorized by topic (ICS = 35.030)

Category (Topic)	Quantity
Technology/Protocol Specific	58
Cryptography	55
Sector specific	32
Privacy	24
Information Security Management System (ISMS)	23
Miscellaneous	18
Authentication	17
Digital signature	13
Protection profile	13
Identity	12
Supply chain	12
Industrial Automation and Control Systems (IACS)	10
Security evaluation	10
Network security	8
Application security	7
Competence	6
Trustworthiness	6
Incident response	5
Cybersecurity	4
Electronic discovery	4
Security assurance	4
Vulnerability management	4
Access control	3
Destruction	3
Non-repudiation	3
Security architecture	3
Evidence	2
Governance	2
Total	361

NIST's practice regarding the identification of its Technical Series publications is inconsistent with the approach adopted by other national and international standards development organizations [43]. For example, it does not appear to employ ICS categories. Current NIST SP 800 series documents were identified by searching the CSRC publications [44]. The search term "800-" was used and results filtered using series "SP" and document status "Final". Filtering eliminated withdrawn documents and current public drafts, yielding a total pf 174 current SP-800 documents. Repeating the search using

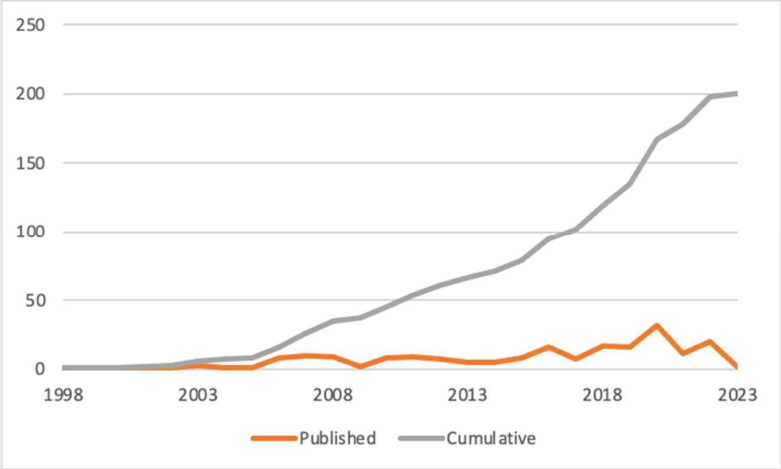

Figure 3 Number of new/revised NIST standards per annum in series SP 800 & SP 1800.

the term "1800-" yielded a further 26 valid current results for the SP 1800 series.

This portfolio of 200 SP 800 and SP 1800 series publications was analyzed to establish publication dates of current versions, see Figure 3, and to categorized documents by the main topic covered, see Table 6. For ease of comparison the same categories have been used in Tables 5 and 6. Allowing for the impact of the Covid pandemic on NIST publishing activity, then in common with international standards bodies there has been a steady increase in standardization activity.

4.3 Assessment of the International Information Security Standards Landscape

Our review of information and cyber security standards published by two national (UK and US) and two international (ISO and IEC) standards organizations, has identified a total of 561 current standards. Of these only the 200 documents published by NIST are free. As discussed in Section 3 only a relatively small portion of these have been subject to academic research. From an end user perspective, it is a time consuming and potentially costly exercise to determine the applicability of individual or groups of standards to a particular enterprise or system context.

Concerns have been expressed about the relevance and quality of many of these standards. For example, Freed [45] cites several criticisms of ISO 27001

Table 6 NIST security-related standards in SP 800 & SP 1800 series – categorized by topic

Category (Topic)	Quantity
Cryptography	32
Technology/Protocol Specific	32
Information Security Management System (ISMS)	21
Miscellaneous	19
Security assurance	16
Identity	15
Sector specific	10
Network security	8
Application Security	7
Access control	6
Incident response	6
Vulnerability management	6
Authentication	3
Digital signature	3
Trustworthiness	3
Cybersecurity	2
Evidence	2
Industrial Automation and Control Systems (IACS)	2
Privacy	2
Security architecture	2
Destruction	1
Security evaluation	1
Supply chain	1
Total	200

made by David Lacey, a security expert instrumental in the development of BS7799, the original source of ISO 27001 content and controls. Lacey expressed concerned about the focus on auditable compliance at the expense of achieving security outcomes. Other concerns expressed by Lacey included the failure to keep up with technology and business development due to slow refresh cycles and the proliferation of standards. The latter criticism is certainly valid given the volume of standards and the rate of publication.

Melancon [46] highlighted two key observations, the evolution of threat agents and the continuing increase in complexity of systems. These observations remain prescient given development over the decade since these were published. Indeed, with increasing interconnectedness of CPS, the increased threats are not a linear progression, they are accelerating. Melancon suggested that the NIST security controls framework was incapable of supporting

our evolved needs as they take a security objective perspective. For example, maintaining confidentiality of information without stating the means to achieve it in operational business processes. Melancon proposed there should be more focus on the security requirements for business processes, e.g., determining whether a given control applies to the business process and if so, how [46].

5 The Linguistic Challenge in IT/Cyber Security Standards

5.1 Background to the Linguistic Challenge

Exploring the linguistic challenge of standardization, Robinson [10] observed that language is a social construct existing within a social system. Bourdieu's concept of habitus considers social systems to comprise communities, where members share perceptions, conceptions and actions performed. Robinson noted that language is always changing [10], and that standards are created by specific 'communities of practice'. Such communities often communicate using specific language, based on shared perceptions, knowledge and skills. Furthermore, Robinson considered that while standards may be written in a common language (e.g., English), the functional language employed may be community specific. Thus, terms are given or adopt community-specific definitions.

This common language with varying meanings becomes problematic when standards are adopted by a wider audience, where the specific concepts, connotations, or use cases may no longer apply. Over time the clarity sought by a community creating a standard, may be compromised through evolution of language and by variations in its interpretation. This may be exacerbated through the loss of nuances when implementation extends beyond the original community. Considering the evolution of computer and information security over the last half century, it is perhaps inevitably that differences will develop in interpretation and usage of language, particularly where a term has a common usage and a specialization in standards.

Linguistic complexity thus arises through fragmented 'communities of practice' creating standards. Robinson [10] opined that standardization may be seen as offering these communities a mechanism for seeking legitimacy for their divergence from existing practices. Robinson also considered that a lack of a domain definition for a community or for standards creates a linguistic challenge. The international standards examined in this research predominantly fall within scope of the ISO/IEC Joint Technical Committee

JCT/1, Information Technology, and Subcommittee SC27, Information security, cybersecurity and privacy protection. Therein lies a potential source of ambiguity, or conflict, as the range of practitioners interested and/or involved in standards creation spans a range of disciplines and organizational domains. For example, the differences and similarities between confidentiality and privacy creating tensions that result in parallel sets of management standards.

Standards development involves subject experts drafting a consensus document which, prior to adoption, is publicly share for review and comment. For topics where standardization is considered necessary and appropriate, the SDOs are reliant upon self-selected experts, who may assume that others share their interpretation of the proposed definitions and normative requirements. As Robinson noted, there is typically no 'right' or 'wrong' language, as perceptions and interpretation may vary according to the context in which a standard is applied. As Alexander [47] noted, consensus is agreement, nothing more, providing no assurance of accuracy, correctness, or feasibility. Thus, different 'communities of practice' may seek to interpret and implement requirements in divergent or contradictory ways. This issue may be exacerbated where organizations seek assurance of compliance with a standard, and the assessors have differing interpretations of the meaning of a standard's clauses.

A further consideration when applying standards is their intended context. For example, there may be industry sector specific issues concerning interpretation and/or application. A standard developed for organizational security of large international companies may be inappropriate for small and medium sized employers. Unfortunately, the relevant implementation domain for standards is often ambiguous or unspecified.

5.2 Examining Definitions of Key Security Goals

Considering the breadth of topics covered by standards in ICS category 35.030, plus NIST SP-800 and SP-1800 series, our third research question explores the consistency of language use. It does so by examining three concepts that feature as security goals since early work on computer security in the 1970s [48]. The goals are confidentiality, availability, and integrity, often referred to by IT security professionals as the 'CIA Triad'.

The methodology used comprised two parts for each of the three terms:

- a search of a representative selection of security literature to examine the definitions in a broad context; and

- a search on the ISO Online Browsing Platform (OBP) to identify definitions of the term in ISO standards.

Results of these searches and subsequent analysis are presented in the Appendices to this paper. The raw data and analysis are being made available in data file.

This analysis of the three terms confidentiality, integrity and availability, demonstrates a lack of consistency of meanings associated with these terms. This is problematic as it creates ambiguity and can result in unforeseen gaps occurring in the design of security measures or controls.

6 Discussion

In addressing our first research question regarding existing research that compared IT security standards, we identified and reviewed 69 relevant papers and found a relatively narrow set of standards were covered by researchers. For example, over seventy percent of the reviewed papers cited ISO 27001/2, which represent two of the two hundred and sixty-one IT security standards published by ISO. We did not locate any systematic analysis of these ISO standards, so existing works have not established the coverage, overlaps, and possible contradictions in this portfolio.

We identified several concerns about the ability of SDOs to keep up with advances in technologies and the proliferation of IT security standards. This is exemplified by the third edition of ISO 27001 [49], superseding the previous 2013 edition. Reviewing latest edition, Malatji [50] noted that IoT devices were not explicitly covered despite their increased deployment in enterprise networks. Malatji proposed that the next update of ISO 27001 should refer to IoT device security but leave the detail to ISO 27400 [51]. Enterprise and Industrial IoT are not new or emerging topics, so this does appear a significant omission given the vulnerabilities these devices can introduced. However, it is a moot point whether such management standards need to, or should, address specific technologies. Perhaps more significant is the impact of such innovations on underlying principles behind such standards, as noted by Freed [45] when reporting Lacey's concerns regarding ISO 27001.

Our second research question established the IT/cyber security standards landscape. In addressing this question, we limited our search to four standards bodies, ISO, IEC, BSI, and NIST. While not exhaustive, the scale of their combined portfolio is illustrative of the volume of relevant publications. The portfolio's size represents a significant challenge for organizations seeking to

identify relevant standards to apply to specific IT systems or scenarios. While ICS is a useful tool for identification of standards relating to IT security (i.e., where ICS = 35.030), it is a very broad classification. As illustrated in Section 3, there is potential for finer classification. We consider further research is required to develop a method that enables potential users to identify relevant standards, their nature, scope, and relationships. This is likely to require a semantically orientated approach.

Our examination of this aggregate portfolio established that the term standard applies to several types of documents. For example, in order of decreasing level of prescription: methods, codes of practice, and guides. Some specify requirements whose conformance can be measured, thus forming the basis for certification schemes. ISO 27001 is an example of such as standard. In a rapidly evolving field like IT security, adoption of certification schemes may significantly lag industry developments and updating of standards [45]. Certification may be cosmetic rather reflect an organization's cyber security posture [52].

Outside of the national and international SDOs, there has been some limited work on digital IoT and digital twin security standardization by the Digital Twin Consortium, an industry membership organization. In our view the criterion for assessing maturity generally lack the rigor of international standards and could therefore be open to subjective interpretation.

Our third research question considered the linguistic challenges posed by inconsistencies in the derivation and definition of terms in standards. We investigated the definition of three key terms or concepts in IT/cyber security – confidentiality, availability and integrity. As illustrated in the Appendices there are a wide range of definitions of these terms. This is problematic as different user communities may have divergent views on the interpretation of the terms and the mechanisms required to achieve them. The situation is further complicated where a standard forms part of an assurance or certification scheme as there may be further interpretation issues between the organization being assessed and the assessors. The language regarding certification can be a potential cause of confusion or misleading interpretation. For example, ISO 27001 and the Common Criteria (ISO 14508) require the scope of evaluation to be clearly identified. The former relates to organizations and their implementation of ISMS, whereas the latter addresses assessing the security of systems in accordance with their target security profile.

Considering ISO 27001 with regards to a CPS, the standard requires the scope of the ISMS to be determined [49], including its boundaries and applicability. The scope is intended to include interfaces and dependencies

between activities performed by the organization, and those that are performed by other organizations [49]. As Culot et al. [52] noted, contemporary IT security practice defends the organizational perimeter, while evolving industry practices (i.e., Industry 4.0, Industrial IoT, and digital twins) blur the physical and digital boundaries. Application of ISO 27001 is therefore problematic with regards to activities performed by second and third parties. Indeed, some security practitioners would argue that this standard is increasingly irrelevant in a hyperconnected environment. In their research Culot et al. [52] found that in respect of standards like ISO 27001, adoption was often perceived as cosmetic, offering limited assurance of business partner's security based on the certification.

Looking beyond the ISO 27000 series of standards, individual ISO and IEC standards may be relevant to securing parts of the system-of-systems. For example, adoption of zones and conduits as advocated by the IEC 62443 standards would aid protection of physical and/or digitally dispersed systems or sub-systems. However, it is important that any approach is holistic, i.e., addresses physical, people, process, and technical security aspects, and that the approach considers the protection of complex CPS and systems-of-systems.

Existing IT security standards are largely based around a narrow set of security goals inherited from a traditional computer security view of systems. We consider that a wider set of security goals is required and propose to investigate what composition of goals might better suit the needs of CPS and complex digital value chains.

7 Conclusions

Our research sought to answer three research questions. We found the scope of existing work is generally limited to comparing standards and controls, and often narrowly focused on comparison of ISO 27001 to other standards, thus ignoring many current IT security standards. Through our searches we identified an IT/cyber security landscape comprising 561 current standards. This large portfolio is potentially difficult for users to navigate and probably contributes to the overreliance on the ubiquitous ISO 27001. To address the security of complex digital value chains, industry should move beyond a checklist approach to security and address the risks and vulnerabilities in these digital ecosystems.

In the applicability and limitations of standards to CPS, in our view there is a significant gap between the needs of organizations and current

IT security standards. The fortress model of a secured perimeter is no longer viable for most businesses, and certainly not for those implementing Industry 4.0, Industrial IoT and digital twins. The technical and business process innovations these bring creates an increasingly porous organizational boundary. To manage the threats and opportunities such innovations create, a fresh approach is required that links business and security goals, and which addresses the functional complexity of the digital value chains.

During our research we identified two areas requiring further work: finer grained classification of IT security standards and an innovative holistic approach linking business and security goals, while addressing the complexity of digital value chains. Working with industry partners we propose to explore these areas.

Appendix A – Evolution and Comparison of Definitions of Availability

Table A.1 illustrates a sample of thirteen definitions of the term availability in the literature, listed in chronological order covering the period 1989 to 2017. The selected sources are typical of those cited in academic literature concerning security of information and systems.

Table A.2 explore the presence of common themes in the selected definitions. There is consensus that timeliness of access to the information, system, or resources. The exception being Firesmith [60] is to a degree circular through its use of available. This definition is also close to the engineering definition of availability, (i.e., MTTF/(MTTF + MTTR). If timeliness is the primary characteristic, the definitions then cover one or more secondary characteristics: accessibility/useability, authorization (of the user), reliability (of access/processing), and denial (of service or withholding access). The latter potentially overlaps with access control, a concept that is also referred to in definitions of the other two goals.

Searching definitions of availability on the ISO online browsing platform a total of 79 definitions were available at the beginning of January 2024. Table A.3 lists the 6 definitions which are used by two or more standards. The results in this table have been conformed to common spelling, for example, treating usable and useable as the same word.

Table A.3 covers definitions adopted by 50 standards, the remaining twenty-nine definitions are listed in Table A.4. Of the definitions in Table A.4, the first and last address timeliness (i.e., "on demand") and the need to be *accessible and useable*. The definition *ability to be in a state to perform as*

Table A.1 Definition of availability

Source	Definition
ISO [53]	The property of being accessible and useable upon demand by an authorized entity
ITSEC [54]	Prevention of the unauthorized withholding of information or resources
OECD [55]	The characteristic of data, information, and information systems being accessible and usable on a timely basis in the required manner
BSI [56]	Ensuring that information and vital services are available to users when required
GASSP [57]	The characteristic of information and supporting information systems being accessible and usable on a timely basis in the required manner
Maconachy et al. [58]	The timely and reliable access to data and information services for authorized users
NIST [59]	A requirement intended to assure that systems work promptly and service is not denied to authorized users
Firesmith [60]	The degree to which a work product is operational and available for use
Avizienis et al. [61]	Readiness for corrective service
Stine et al. [62]	Ensuring timely and reliable access to and use of information
NIST [63]	Ensuring timely and reliable access to and use of information
Zafar et al. [64]	Means the system is available continuously to each authorised user without disruption
ISO [65]	Property of being accessible and usable upon demand by an authorized entity

Table A.2 Analysis of common themes in definitions of availability

Source	Timeliness	Accessible & Useable	Authorisation	Reliable	Denial/ Withholding
ISO	x	x	x		
ITSEC			x		x
OECD	x	x			
BSI	x				
GASSP	x	x			
Maconachy et al.	x		x	x	
NIST	x		x		x
Firesmith				x	
Avizienis et al.	x				
Stine et al.	x	x		x	
NIST	x	x		x	
Zafar et al.	x		x	x	x
ISO	x	x	x		

Table A.3 Definition of availability used by two or more iso standards [Source: iso.org/obp]

Definition	Count
Property of being accessible and useable upon demand by an authorized entity	30
ability to be in a state to perform as required	7
Extent to which the infrastructure, assets, resources and employees of a water utility enable effective provision of services to users according to specified performances	6
Ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided	3
Degree to which content, documents, facilities or services are actually provided by the library at the time required by users	2
Property of data or of resources being accessible and usable on demand by an authorized entity	2

required appears somewhat ambiguous. Having an ability suggests that the related entity could, or may, be able to perform, and not that it will do so when required. The definition an *ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided* is particularly specific about the characteristics of availability and would be useful in situations where availability is critical. Overall, definitions listed in Table A.4 illustrate the diversity of interpretations of this goal.

Table A.4 Definition of Availability used by a single ISO standard [Source: iso.org/obp]

Ability of a functional unit to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided
Probability, at any time, that the measuring system, or a measuring instrument forming part of the measuring system, is functioning according to specifications
Period(s) during which a facility or service is serviceable
Ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided
Degree to which content, documents, facilities, or services are actually provided by the library at the time required by users
Ability of an application object to perform its required function at an agreed instant or over an agreed period of time
Fraction of the total time that the automatic measuring system is operational and for which valid measuring data are available

(*Continued*)

Table A.4 Continued

Ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided
Probability of a repairable item being operable when it is required to operate. Availability is the total characteristics of reliability, serviceability and accessibility of the item. Availability can be detailed as instantaneous availability and mean availability.
Property of data or of resources being accessible and usable on demand by an authorized entity
Ability of a PCC plant integrated with the power plant to be in a state to perform as required under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided
Prevention of the unauthorized withholding of information or resources
Degree to which materials, facilities or information services are actually provided by an information and documentation organization at the time they are required by information users
Capability of a product to be operational and accessible when required for use
Extent to which the system/structure/equipment is capable of retaining its functional integrity
Capability of a product to provide a stated function if demanded, under given conditions over its defined lifetime
Percentage of the full measurement period during which the measurement chain is available for making measurements
Capability of a product to provide a stated function if demanded, under given conditions over its defined lifetime
Periods during which a facility or service is serviceable
Property of being accessible and useable upon demand by an authorized entity.
Probability that a machine will, when used under specified conditions, operate satisfactorily and effectively
Share of the total time that the CGS is available to produce electric power, heating and/or cooling as required during a defined period, normally a calendar year
1. Ability of a service or service component to perform its required function at an agreed instant or over an agreed period of time.
2. Degree to which a system or component is operational and accessible when required for use
Property of being accessible and useable upon demand by an authorized entity
Ability of a treatment technology to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the Required external resources are provided
Degree to which a cloud service is accessible and usable upon demand by an authorized entity
State of being able to perform the required function
Degree to which a system, product or component is operational and accessible when required for use
Degree to which an IT service is available to users when needed

Appendix B – Evolution and comparison of definitions of Integrity

Table B.1 illustrates a sample of fourteen definitions of the term integrity in the literature, listed in chronological order covering the period 1989 to 2017. The selected sources are typical of those cited in academic literature concerning security of information and systems.

Table B.1 Definition of integrity in selected literature

Source	Definition
ISO	The property that data has not been altered or destroyed in an unauthorized manner
ITSEC	Prevention of the unauthorized modification of information
OECD	The characteristic of data and information being accurate and complete and the preservation of accuracy and completeness
BSI	Safeguarding the accuracy and completeness of information and computer software
GASSP	The characteristic of information being accurate and complete and the information systems' preservation of accuracy and completeness
Maconachy et al.	The quality of an information system reflecting logical correctness and reliability of an operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.
NIST (2001)	Data integrity is the property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit. System integrity is the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation
Firesmith	The degree to which components are protected from intentional and unauthorized corruption. Further broken down into data, hardware, personnel and software
Avizienis et al.	Absence of improper system alteration
Stine et al.	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
NIST	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Zafar et al.	Preventing the unauthorized modification or alteration of information and ensures the originality of information
NIST	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
ISO	Property of accuracy and completeness

Table B.2 Analysis of common themes in definitions of Integrity in selected literature

Source	Altered/ Modified	Destroyed	Unauthorized/ Improper	Accurate & Complete	Non-repudiation	Authenticity
ISO	x	x	x			
ITSEC	x		x			
OECD				x		
BSI				x		
GASSP				x		
Maconachy et al.						
NIST (2001)	x		x			
Firesmith	x	x	x			
Avizienis et al.	x		x			
Stine et al.	x	x	x		x	x
NIST	x	x	x		x	x
Zafar et al.	x	x	x			
NIST	x	x	x		x	x
ISO				x		

Table B.2 explores the presence of common themes in the selected definitions. There is some consensus, from eight sources, that integrity relates to the prevention of unauthorized (or improper) modification or destruction of information (data), although three source extended the definition to also address changes to systems (hardware and/or software). However, five of the definitions refer to accuracy and completeness rather than authorization and modification/destruction. It is interesting to note the inclusion of non-repudiation (i.e., assurance that a transaction is valid) and authenticity by three definitions. Inclusion of authenticity in the definition of integrity is debatable. It potentially leads to consideration of the role of provenance in information systems and CPS, i.e., the authenticity, origin, and history of objects, whether digital or physical in nature.

Searching for definitions of integrity on the ISO online browsing platform a total of 56 definitions were available at the beginning of January 2024. Table B.3 lists the 7 definitions which are used by two or more standards. These cover 25 of the 56 standards, the remaining thirty-one definitions are listed in Table B.4. The results in Table A-7 split in a similar fashion to those in Table A-5, with some addressing accuracy and completeness and others focusing on preventing unauthorized changes or destruction. The definitions listed in Table B.4 illustrate the diversity of interpretations of the concept of integrity.

Table B.3 Definition of integrity used by two or more ISO standards [Source: iso.org/obp]

Definition	Count
Property of accuracy and completeness	8
Property of safeguarding the accuracy and completeness of assets	5
Property that data has not been altered or destroyed in an unauthorized manner	3
Property of protecting the accuracy and completeness of assets	2
Measure of the trust that can be placed in the correctness of the information supplied by a navigation system and that includes the ability of the system to provide timely warnings to users when the system should not be used for navigation	2
Quality of being complete and unaltered	3
Property that the parameter(s) of interest, information or content of the sample container has not been altered or lost in an unauthorized manner or subject to loss of representativeness	2

Table B.4 Definition of integrity used by a single ISO standard [Source:iso.org/obp]

Capability of a product to ensure that the state of its system and data are protected from unauthorized modification or deletion either by malicious action or computer error
Attribute of a document whose content is unimpaired
Completeness in content and structure
Property of being designed such that any modification of the electronically stored information, without proper authorization, is not possible
Condition of guarding against improper modification or destruction of information
Attribute of a document whose content is complete and unaltered
Degree to which a system, product or component prevents unauthorized access to, or modification of, computer programs or data
Property that data has not been modified or deleted in an unauthorized and undetected manner
Degree to which an IT service prevents unauthorized access to or modification of data whether accidently or intentionally
Proof that the message content has not altered, deliberately or accidentally in any way, during transmission
Designed such that any modification of the electronically stored information, without proper authorization, is not possible
Property of data whose accuracy and consistency are preserved regardless of changes made
Internal consistency or lack of corruption in electronic data
Ability of an application to function as designed within a BACS
Property of accuracy and completeness
Property of safeguarding the accuracy and completeness of information and processing methods

(*Continued*)

Table B.4 Continued

Property that information is not altered in any way, deliberately or accidentally
Property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner
Property whereby data have not been altered in an unauthorized manner since they were created, transmitted or stored
Property that data have not been altered or destroyed in an unauthorized manner
Degree to which a system, product, or component prevents unauthorized access to, or modification of, computer programs or data
Safeguarding the accuracy and completeness of information and processing methods
Proof that the message content has not altered, deliberately or accidentally in any way, during transmission
Quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data
Proof that the message content has not been altered, deliberately or accidentally in any way, during transmission
Reliability of data that are as they were created according to the required verification parameters
Proof that the message content has not been altered, deliberately or accidentally, in any way during transmission
State of an artefact that has not been altered, deliberately or accidentally
State of immutability of information
Property whereby data have not been altered in an unauthorized manner since they were created, transmitted, or stored
Property of being able to safeguard the accuracy and the completeness of assets.

Appendix C – Evolution and comparison of definitions of Confidentiality

Table C.1 illustrates a sample of fourteen definitions of the term availability in the literature, listed in chronological order covering the period 1989 to 2017. The selected sources are typical of those cited in academic literature concerning security of information and systems.

Searching for definitions of confidentiality on the ISO OBP, a total of 68 definitions were available at the beginning of January 2024. Table C.2 lists the three definitions which are used by two or more standards. These cover 46 of the 68 standards, the remaining 22 definitions are listed in Table C.3. Whilst the phrasing of the definitions in Table A-7 varies, they all address the issue of unauthorized access, whether the information is *made available*

or *disclosed*. The third definition is weaker than the first two as it could be interpreted as only relating to access by one or more people, whereas the other definitions address unauthorized access, by *entities, or processes*, i.e., organizations and/or other systems. The definitions listed in Table C.3 illustrate the diversity of interpretations of the concept of confidentiality.

Table C.1 Definition of Confidentiality

Source	Definition
ISO	The property that information is not made available or disclosed to unauthorized individuals, entities or processes
ITSEC	Prevention of the unauthorized disclosure of information [DTI:1991]
OECD	The characteristic of data and information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner [OECD:1992]
BSI	Protecting sensitive information from unauthorized disclosure or intelligible interception [BSI:1995]
GASSP	The characteristic of information being disclosed only to authorized persons, entities, and processes at authorized times and in the authorized manner [I2SF:1999]
Maconachy et al.	The assurance that information is not disclosed to unauthorized persons, processes or devices.
NIST (2001)	The requirement that private or confidential information not be disclosed to unauthorized individuals
Firesmith	The degree to which sensitive information is not disclosed to unauthorized parties
Avizienis et al.	The absence of unauthorized disclosure of information
Stine et al.	Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information
NIST	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [NIST:2010]
Zafar et al.	Preserving the privacy of information by protecting invalid access to it
NIST	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
ISO	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes – ISO 27000 [BSI, 2017a]

Table C.2 Definition of Confidentiality used by two or more ISO standards [Source: iso.org/obp]

Definition	Count
property that information is not made available or disclosed to unauthorized individuals, entities, or processes	42
property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes, or other entities	2
degree to which a product or system ensures that data are accessible only to those authorized to have access	2

Table C.3 Definition of Confidentiality used by a single ISO standard [Source:iso.org/obp]

Property that information is not made available or disclosed to unauthorized individuals, entities or processes
Process that ensures that information is not made available or disclosed to unauthorized individuals, entities or processes
Condition in which information is shared or released in a controlled manner
Access restricted to some defined level of differential-identity authentication
Restriction of access to data and information to individuals who have a need, a reason and permission for access
Assurance that communicated data remain private to the parties for whom the data are intended
Security service that protects data from unauthorized disclosure
Capability of a product to ensure that data are accessible only to those authorized to have access
Process that ensures that information is accessible only to those authorized to have access
Degree to which a cloud service ensures that data are accessible only to those authorized to have access
Property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes or other entities
Property that information is not made available or disclosed to unauthorised entities
Property that information is not available or disclosed to unauthorized individuals, entities or processes
Status accorded to data or information indicating that it is sensitive for some reason, and that therefore it needs to be protected against theft or improper use and must be disseminated only to individuals or organizations authorized to have it
Protection of information from unauthorized disclosure
Property whereby information is not disclosed to unauthorized parties
Degree to which an IT service ensures that data are accessible only to those authorized to have access
Requirement that information, materials and data collected are protected from unauthorized access

(*Continued*)

Table C.4 Continued

Preserving authorized restrictions on, and preventing unauthorized access to information
The protection of information from unauthorized disclosure
Prevention of information leakage to non-authenticated individuals, parties or processes
Prevention of information leakage to non-authenticated individuals, parties, and/or processes

References

[1] Leyden, J. (2013) "Drug gang hacks into Belgian seaport, cops seize TONNE of smack." The Register. Available: https://www.theregister.com/2013/06/18/drug_smugglers_using_hackers/.

[2] EC3 (2013) "Hackers deployed to facilitate drugs smuggling." Cyber Bits, European Cybercrime Centre, Europol, The Hague. Intelligence Notification 004-2013. Available: https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf.

[3] Pang, T.Y.; Pelaez Restrepo, J.D.; Cheng, C.-T.; Yasin, A.; Lim, H.; Miletic, M. (2021) "Developing a Digital Twin and Digital Thread Framework for an 'Industry 4.0' Shipyard." Applied Science, 11, 1097. DOI: 10.3390/app11031097.

[4] Karie, N.M., Sahri, N.M., Yang, W., Valli, C. and Kebande, V.R. (2021) "A review of security standards and frameworks for IoT-based smart environments." IEEE Access, vol. 9, pp. 121975–121995, DOI: 10.1109/ACCESS.2021.3109886.

[5] Sommestad, T., Ericsson, G.N. and Nordlander, J., (2010, July) "SCADA system cyber security – A comparison of standards." IEEE PES General Meeting, Minneapolis, MN, USA, pp. 1–8, DOI: 10.1109/PES.2010.5590215.

[6] Zhou, X., Xu, Z., Wang, L. and Chen, K. (2017, April) "What should we do? A structured review of SCADA system cyber security standards." In: 4th International Conference on Control, Decision and Information Technologies (CoDIT), Barcelona, Spain, pp. 0605–0614, DOI: 10.1109/CoDIT.2017.8102661.

[7] Linnosmaa, J., Papakonstantinou, N., Malm, T., Kotelba, A. and Pärssinen, J. (2021, November) "Survey of cybersecurity standards for nuclear instrumentation and control systems." In: International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2021: Online. Okayama University

[8] Arora, V., 2010. Comparing different information security standards: COBIT vs. ISO 27001. BSI Stand, pp. 7–9. Available: https://varunarora.com/assets/iso27001-vs-cobit/paper.pdf.

[9] Glavič, P. (2021) "Special Issue: Feature Papers to Celebrate the Inaugural Issue of Standards." Standards, 1(1), pp. 17–18; DOI: 10.3390/standards1010003.

[10] Robinson, R.C. (2022) "The Linguistic Challenge for Standards." Standards, 2, pp. 449–459. DOI: 10.3390/standards2040030.

[11] ISO (2000) "Information technology. Code of practice for information security management." International Organization for Standardization (ISO), Geneva, Switzerland.

[12] ISO (2005) "Information technology – Security techniques – Code of practice for information security management." International Organization for Standardization (ISO), Geneva, Switzerland.

[13] Frangopoulos, E.D. and Eloff, M.M. (2004, June) "A Comparative Study of Standards and Practices Related to Information Security Management." In ISSA (pp. 1–15).

[14] Evans, R.P., Hill, R.C. and Rodriquez, J.G. (2005) "A Comparison of Cross-Sector Cyber Security Standards." Idaho National Laboratories. Idaho National Labs Rep. INL/EXT-05-00656. DOI: 10.2172/911585.

[15] Trappey, A.J., Trappey, C.V., Govindarajan, U.H., Chuang, A.C. and Sun, J.J. (2017) "A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0." Advanced Engineering Informatics, vpl. 33, pp. 208–229. DOI: 10.1016/j.aei.2016.11.007.

[16] Leszczyna, R. (2018) "A review of standards with cybersecurity requirements for smart grid." Computers & Security, vol. 77, pp. 262–276. DOI: 10.1016/j.cose.2018.03.011.

[17] Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S., (2010) "A security standards' framework to facilitate best practices' awareness and conformity." Information Management & Computer Security, 18(5), pp. 350–365. DOI: 10.1108/09685221011095263.

[18] Beckers, K., Côté, I., Fenz, S., Hatebur, D., Heisel, M. (2014). A Structured Comparison of Security Standards. In: Heisel, M., Joosen, W., Lopez, J., Martinelli, F. (eds) Engineering Secure Future Internet Services and Systems. Lecture Notes in Computer Science, vol. 8431. Springer, Cham. DOI: 10.1007/978-3-319-07452-8_1.

[19] Sunyaev, A. (2011). "Designing a Security Analysis Method for Healthcare Telematics in Germany." In: Health-Care Telematics in Germany. Gabler. DOI: 10.1007/978-3-8349-6519-6_5.

[20] Paudel, S., Tauber, M., Wagner, C., Hudic, A. and Ng, W.K. (2014, December) "Categorization of standards, guidelines and tools for secure system design for critical infrastructure it in the cloud." In: 2014 IEEE 6th International Conference on Cloud Computing Technology and Science, pp. 956–963. DOI: 10.1109/CloudCom.2014.172.

[21] Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R.H. and Bashir, M.N. (2017, June) "Cloud standards in comparison: Are new security frameworks improving cloud security?" In: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), Honololu, HI, USA. pp.50-57, DOI: 10.1109/CLOUD.2017.16.

[22] CSA (2016) "'The Treacherous Twelve' Cloud Computing Top Threats in 2016." Cloud Security Alliance, Bellingham, WA. Available: https://cloudsecurityalliance.org/artifacts/the-treacherous-twelve-cloud-computing-top-threats-in-2016/.

[23] de Franco Rosa, F., Jino, M., Bueno, P.M.S. and Bonacin, R. (2018, April) "Coverage-based heuristics for selecting assessment items from security standards: a core set proposal." In: 2018 Workshop on Metrology for Industry 4.0 and IoT, Brescia, Italy. pp. 192–197, DOI: 10.1109/METROI4.2018.8428307.

[24] de Franco Rosa, F., Jino, M., Bonacin, R. (2018). "Towards an Ontology of Security Assessment: A Core Model Proposal." In: Latifi, S. (ed) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol. 738. Springer, Cham. DOI: 10.1007/978-3-319-77028-4_12.

[25] Stouffer, K. (2004), System Protection Profile–Industrial Control Systems Version 1.0, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD. DOI: 10.6028/NIST.IR.7176.

[26] Piggin, R.S.H. (2013, June) "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security." In: IET Conference on Control and Automation 2013: Uniting Problems and Solutions, Birmingham, pp. 1–6, DOI: 10.1049/cp.2013.0001.

[27] Tsohou, A., Kokolakis, S., Lambrinoudakis, C. and Gritzalis, S. (2010a) "Information systems security management: a review and a classification of the ISO standards." In: Sideridis, A.B., Patrikakis, C.Z. (eds)

Next Generation Society. Techno-logical and Legal Issues. e-Democracy 2009. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol.26. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-11631-5_21.

[28] Mussmann, A., Brunner, M. and Breu, R. (2020, March) "Mapping the State of Security Standards Mappings." In: Wirtschaftsinformatik (zentrale tracks), pp. 1309–1324. DOI: 10.30844/wi_2020_l4-mussmann.

[29] Milicevic, D. and Goeken, M. (2010) "Ontology-based evaluation of ISO 27001." In: Cellary, W., Estevez, E. (eds) Soft-ware Services for e-World. I3E 2010. IFIP Advances in Information and Communication Technology, vol. 341. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-16283-1_13.

[30] ISO (2020) Information technology – Security techniques – Information security management systems – Overview and vocabulary. International Organization for Standardization (ISO), Geneva, Switzerland.

[31] Ehrlich, M., Trsek, H., Wisniewski, L. and Jasperneite, J. (2019, October) "Survey of Security Standards for an automated Industrie 4.0 compatible Manufacturing." In: ECON 2019 – 45th Annual Conference of the IEEE Industrial Electronics Society, Lisbon, Portugal. pp. 2849–2854, DOI: 10.1109/IECON.2019.8927559.

[32] Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K. and Stantchev, V. (2016) "Security management standards: A mapping." Procedia Computer Science, vol. 100, pp. 755–761. DOI: 10.1016/j.procs.2016.09.221.

[33] ISO (2013) Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization (ISO), Geneva, Switzerland.

[34] Barlette, Y. and Fomin, V.V. (2010) "The adoption of information security management standards: A literature review." In: Information Resource Management Association (Ed.), Information Resources Management: Concepts, Methodologies, Tools and Applications. pp. 69–90. IGI Global. DOI: 10.4018/978-1-61520-965-1.ch104.

[35] Taherdoost, H., (2022) "Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview." Electronics, 11(14), p. 2181. DOI: 10.3390/electronics11142181.

[36] ISO (2015a) "International Classification for Standards." International Organization for Standardization (ISO), Geneva, Switzerland. Seventh

edition, ISBN 978-92-67-10652-6 Available online: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/international_classification_for_standards.pdf.

[37] BSI "British Standards Online." British Standards, London. Available online: https://bsol.bsigroup.com/.

[38] ISO. 35.030 IT Security Including encryption. International Organization for Standardization, Geneva, Switzerland. Avail-able online: https://www.iso.org/ics/35.030/x/.

[39] IEC Webstore. International Electrotechnical Commission, Geneva. Available: https://webstore.iec.ch/advsearchform.

[40] IEC (2018) "Guide 120 - Security aspects - Guidelines for their inclusion in publications." International Electrotechnical Commission, Geneva.

[41] NIST (2018a) "NIST Special Publication 800-series General Information." National Institute of Standards and Technology, Gaithersburg, MD, USA. Available online: https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information.

[42] NIST (2018b) "NIST Special Publication 1800-series General Information." National Institute of Standards and Technology, Gaithersburg, MD, USA. Available online: https://www.nist.gov/itl/publications-0/nist-special-publication-1800-series-general-information.

[43] NIST (2021) "Publication Identifier Syntax for NIST Technical Series Publications." Information Services Office, National Institute of Standards and Technology, Gaithersburg, MD, USA. Available online: https://www.nist.gov/document/publication-identifier-proposal.

[44] CSRC Current Publications. Computer Security Resource Center (CSRC), National Institute of Standards and Technology, Gaithersburg, MD, USA. Available online: https://csrc.nist.gov/publications/search.

[45] Freed, A.M. (2013) "David Lacey on What's Wrong with Today's ISO27k Standards." The State of Security. Trip-wire.com Available online: https://web.archive.org/web/20131014052141/https://www.tripwire.com/state-of-security/regulatory-compliance/david-lacey-whats-wrong-todays-iso27k-standards/.

[46] Melancon, D. (2013) "NIST: It's Time to Abandon Control Frameworks as We Know Them." The State of Security, Trip-wire.com. Available online: https://web.archive.org/web/20131009090221/http://www.tripwire.com/state-of-security/security-data-protection/nist-its-time-to-abandon-control-frameworks-as-we-know-them/.

[47] Alexander, A. "When Consensus Is a Bad Way to Decide". Available online: https://www.theunion.com/news/twi/when-consensus-is-a-bad-way-to-decide/.

[48] DSBTFCS (1970) "Security Controls for Computer Systems." Defense Science Board Task Force on Computer Security. Available online: https://www.rand.org/pubs/reports/R609-1.html.

[49] ISO (2022a) "27001 Information security, cybersecurity and privacy protection. Information security management system. Requirements." International Organization for Standardization (ISO), Geneva, Switzerland.

[50] Malatji, M., (2023, January) "Management of enterprise cyber security: A review of ISO/IEC 27001:2022." In 2023 International Conference On Cyber Management And Engineering (CyMaEn), Bangkok, Thailand, pp. 117–122, DOI: 10.1109/CyMaEn57228.2023.10051114.

[51] ISO (2022b) "27400 Cybersecurity – IoT security and privacy – Guidelines." International Organization for Standardization (ISO), Geneva, Switzerland.

[52] Culot, G., Fattori, F., Podrecca, M., and Sartor, M. (2019, Sept.) "Addressing Industry 4.0 Cybersecurity Challenges," in IEEE Engineering Management Review, vol. 47(3), pp. 79–86, DOI: 10.1109/EMR.2019.2927559.

[53] ISO (1989) "ISO 7498-2 "Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture" International Organization for Standardization (ISO), Geneva.

[54] DTI (1991). "Information Technology Security Evaluation Criteria (ITSEC)." Version 1.2. Department for Trade and Industry, London.

[55] OECD (1992). Guidelines for the Security of Information Systems. Paris: OECD Organization for Economic Cooperation and Development. Available: http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.

[56] BSI (1995) B7799-1:1995 Information security management - Part 1. Code of practice for information security management systems. London: British Standards Institution. p1.

[57] I2SF (1999) "Generally Accepted System Security Principles (GASSP) – Version 2.0", June 1999, International Information Security Foundation, USA.

[58] Maconachy, W.V., Schou, C.D., Ragsdale, D. and Welch, D., (2001, June) "A model for information assurance: An integrated approach."

In Proceedings of the 2001 IEEE workshop on information assurance and security (Vol. 310, pp. 5–6). United States Military Academy, West Point. IEEE. Available: https://os.ecci.ucr.ac.cr/ci0122/Temas/Semana-02/MSRW-Paper.pdf.

[59] Stoneburner, G. (2001), Underlying Technical Models for Information Technology Security, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151250 (Accessed January 13, 2024).

[60] Firesmith, D. G., (2003) "Common Concepts Underlying Safety, Security, and Survivability Engineering." Software Engineering Institute, Carnegie Mellon University, Technical Note CMU/SEI-2003-TN-033. DOI: 10.1184/R1/6572621.v1.

[61] Avizienis, A., Laprie, J.C., Randell, B. and Landwehr, C. (2004) "Basic concepts and taxonomy of dependable and secure computing." IEEE transactions on dependable and secure computing, 1(1), pp. 11–33. DOI: 10.1109/TDSC.2004.2.

[62] Stine, K., Kissel, R., Barker, W., Fahlsing, J. and Gulick, J., (2008). "Guide for mapping types of information and information systems to security categories." NIST Special Publication (SP) 800-60 V.1, R.1. National Institute of Standards and Technology, Gaithersburg, MD. DOI: 10.6028/NIST.SP.800-60v1r1.

[63] NIST (2010) Guide for Applying the Risk Management Framework to Federal Information Systems. Special Publication 800-37 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology.

[64] Zafar, N., Arnautovic, E., Diabat, A. and Svetinovic, D., 2014. "System security requirements analysis: A smart grid case study." Systems Engineering, 17(1), pp. 77–88. DOI: 10.1002/sys.21252.

[65] ISO (2018) "ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary."

Biographies

Hugh Boyes (Member, IEEE) received the bachelor's degree in biomedical electronics from the University of Salford in 1982, and the master's degree in business administration from Brunel University in 1995. Hugh is currently a doctoral candidate in WMG at the University of Warwick. He is a Chartered Engineer and currently works as an information security consultant and part-time Associate Research Fellow at Loughborough University. His research areas include the security of cyber physical systems and of digital twins.

Matthew D. Higgins (Senior Member, IEEE) is a Reader at the University of Warwick, where he leads WMG's Connectivity and Communications Technology Research Group within its Intelligent Vehicles Directorate. His research interests span 5G and Beyond, Core Networking, IEEE 802.3xx, GNSS, and Timing, with applications to both the Automotive and Manufacturing domains. Coupled with an overarching motivation to ensure ongoing resilience of the domain is considered, Matthew leads many high-value collaborative projects funded through EPSRC, Innovate UK, and HVMC, as well as also leading multiple projects funded directly by industry.