

URL	https://www.computer.org
Country of HQ location	US
Geographic Scope	International
Type	Academic (not for profit)

Risultati di questa iniziativa sono libri, conferenze, pubblicazioni relative a conferenze, riviste, corsi on-line, certificazioni di sviluppo software, standard e riviste tecniche.

Risultati più rilevanti:

Good Practice	<p>Guide to the Software Engineering Body of Knowledge (SWEBOK), la guida descrive le conoscenze generalmente accettate in materia di ingegneria del software. Le sue 15 aree di conoscenza (knowledge areas) riassumono i concetti di base e includono un elenco di riferimento per informazioni più dettagliate.</p> <p>Enterprise Information Technology Body of Knowledge (EITBOK) Guide. Un compendio di descrizioni di alto livello delle aree di conoscenza (knowledge areas) che sono generalmente necessarie per il buon funzionamento della tecnologia dell'informazione (IT).</p>
Standard	<p>Software & Systems Engineering Standards Committee (S2ESC)</p> <p>Formal Liaisons with ISO/IEC JTC1/SC7.</p>

5.1.4 International Organisation for Standardization (ISO)

ISO è il più grande sviluppatore e editore al mondo di standard internazionali. Industrie ed esperti del settore generalmente contribuiscono come membri dei comitati tecnici ISO proponendo nuove normative che devono essere approvate almeno dal 70% dei membri ISO.

Il comitato tecnico che opera nell'ambito degli standard IT è il JTC 1 che, a sua volta, è organizzato in 22 sottocomitati che coprono aree specifiche. Si riporta di seguito un sottoinsieme significativo:

- ISO / IEC JTC 1 / SC 7: Ingegneria del software e dei sistemi;
- ISO / IEC JTC 1 / SC 22: Linguaggi di programmazione, compresi ambienti e interfacce software di sistema;
- ISO / IEC JTC 1 / SC 27: Sicurezza delle informazioni, sicurezza informatica e protezione della privacy;
- ISO / IEC JTC 1 / SC 38: Cloud Computing e piattaforme distribuite;
- ISO / IEC JTC 1 / SC 41: Internet of Things e tecnologie correlate;
- ISO / IEC JTC 1 / SC 42: Intelligenza artificiale.

Relativamente agli ambiti SSE troviamo:

- pubblicazione di rapporti tecnici e standard:
 - ISO / IEC TR 15026-1: 2013, ISO / IEC TR 24731-1: 2007, ISO / IEC TR 24772: 2013, ISO / IEC 15408 e ISO / IEC 18405
- 2 progetti in corso.

URL	https://www.iso.org
Geographic Scope	International
Type	Network of national standards institutes

Risultati più rilevanti:

ISO/IEC JTC 1/SC 7	<u>ISO/IEC 15026-1:2019 Systems and software engineering -- Systems and software assurance -- Part 1: Concepts and vocabulary</u>
ISO/IEC JTC 1/SC 22	<p><u>ISO/IEC TR 24731-1:2007</u> Information technology - Programming languages, their environments and system software interfaces - Extensions to the C library - Part 1: Bounds-checking interfaces.</p> <p>Specifica una serie di estensioni del linguaggio di programmazione C, specificato dalla norma internazionale ISO/IEC 9899: 1999. Queste estensioni possono essere utili nella mitigazione delle vulnerabilità di sicurezza nei programmi.</p> <p><u>ISO/IEC TR 24731-2:2010</u> Information technology — Programming languages, their environments and system software interfaces — Extensions to the C library — Part 2: Dynamic Allocation Functions.</p> <p>Fornisce funzioni alternative per la libreria C che favoriscono la programmazione sicura.</p> <p><u>ISO/IEC TR 24772:2013</u> Information technology - Programming languages - Guidance on avoiding vulnerabilities in programming languages through language selection and use.</p> <p>Specifica le vulnerabilità del linguaggio di programmazione software da evitare nello sviluppo di sistemi in cui è richiesto un comportamento sicuro ai fini security/safety, mission critical e software business-critical. In generale, questa guida è applicabile al software sviluppato, rivisto, o mantenuto per qualsiasi applicazione. Le vulnerabilità sono descritte in modo generico, applicabili a una vasta gamma di linguaggi di programmazione.</p> <p>Questa guida può essere anche utilizzata dagli sviluppatori per produrre o selezionare gli strumenti di valutazione del codice sorgente capaci di scoprire ed eliminare alcuni costrutti che potrebbero portare alla vulnerabilità del software o per selezionare un linguaggio di programmazione che consenta di evitare i problemi attesi.</p>