

### List of Security Standards/Frameworks

ISO/IEC 27001/2	International Organization for Standardization 2700X standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls, taking into consideration the organization's information security risk environment(s). ISO charges for access to this standard. <a href="https://www.iso.org/standard/54533.html">https://www.iso.org/standard/54533.html</a>
NIST 800-53/CSF	The National Institute of Standards and Technology's (NIST) Special Publication 800-53 provides controls for federal information systems, but it can be employed by commercial entities. NIST offers the cybersecurity framework (CSF), which incorporates 800 and the Federal Information Processing Standard. There is no charge for access to the standard. <a href="https://nvd.nist.gov/800-53">https://nvd.nist.gov/800-53</a>
CIS 20	The Center for Internet Security maintains a standard of 20 controls, originally developed by SANS. There is no charge for access to this standard. <a href="https://www.cisecurity.org/controls/">https://www.cisecurity.org/controls/</a>
ISACA COBIT 5	The Information Systems Audit and Control Association offers the COBIT framework for information security. Represented to align with ISO 27000 series, Information Security Forum standard, and BMIS. There is a charge for access to the standard. <a href="http://www.isaca.org/COBIT/pages/default.aspx">http://www.isaca.org/COBIT/pages/default.aspx</a>
ISF	The Information Security Forum's Standard of Good Practice provides controls and guidance on current and emerging security topics. The Standard and its corresponding ISF Benchmark align with ISO 27002, COBIT 5, CIS 20, NIST, and PCI-DSS. <a href="https://www.securityforum.org/tool/the-isf-standardrmation-security/">https://www.securityforum.org/tool/the-isf-standardrmation-security/</a>
DISA	The Defense Information Security Agency provides security standards including Control Correlation Identifiers (CCIs), Security Requirements Guides (SRGs), Security Technical Implementation Guides (STIGs), and mobile code. <a href="http://www.disa.mil/~media/Files/DISA/News/Conference/2016/AFCEA-Symposium/3-McKinney_Security%20Standards.pdf">http://www.disa.mil/~media/Files/DISA/News/Conference/2016/AFCEA-Symposium/3-McKinney_Security%20Standards.pdf</a>
ITIL	Maintained by Axelos, the Information Technology Infrastructure Library is directed to IT Service Management. Aligned with the ISO 20000 series, it is published as a series of five core volumes, each covering a different ITSM lifecycle stage. There is a charge for access to this standard. <a href="https://www.axelos.com/best-practice-solutions/itil/what-is-itil">https://www.axelos.com/best-practice-solutions/itil/what-is-itil</a>
PCI-DSS	A joint venture by the major credit card companies, the Payment Card Industry security council's Data Security Standard is a set of policies and procedures intended to improve the security of card transactions.

	<p>Compliance is mandated by the credit card companies. In addition, some state laws either refer to it, or mirror certain aspects of the standard.</p> <p><a href="https://www.pcisecuritystandards.org/pci_security/">https://www.pcisecuritystandards.org/pci_security/</a></p>
OWASP	<p>The Open Web Application Security Project offers a number of resources to improve the security of web applications, including the popular OWASP Top 10. There is no charge for access to the OWASP Top 10.</p> <p><a href="https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a></p>
BSIMM	<p>The Building Security in Maturity Model is directed to software security, and offers a framework used to organize a number of activities to help manage and measure enterprise security initiatives. There is no charge for access to the framework. <a href="https://www.bsimm.com/framework.html">https://www.bsimm.com/framework.html</a></p>
CSA 4.0	<p>The Cloud Security Alliance offers the Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 for the purpose of improving security and mitigating risk in the adoption of cloud computing technologies. <a href="https://cloudsecurityalliance.org/guidance/#_overview">https://cloudsecurityalliance.org/guidance/#_overview</a></p>
ILTA	<p>The International Legal Technology Association's LegalSEC provides the legal community with guidelines for risk-based information security programs. Certain tools are available to the public at no charge. <a href="https://www.iltanet.org/resources/legalsec">https://www.iltanet.org/resources/legalsec</a></p>