SmartSuite

Framework / Software Security / ISO Industry Standards

UL 2900-1

UL 2900-1 specifies cybersecurity requirements for software in network-connectable products to reduce vulnerabilities and ensure secure operation.

What it is

UL 2900-1 — Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements is a cybersecurity standard that establishes baseline requirements for the security of software in network-connectable products. The framework aims to reduce cybersecurity risks by mandating controls that address vulnerabilities and threats throughout a product's software lifecycle.

Published by UL Solutions, UL 2900-1 is used by manufacturers, product developers, and compliance professionals seeking to certify or assess the cybersecurity posture of connected devices. The standard covers areas such as secure software development, vulnerability testing, data protection, access control, and security update mechanisms, ensuring robust risk management across diverse product categories.

At a glance

PUBLISHER Underwriters Laboratories (also known as UL or UL Solutions)	TYPE Standard	VERSION 2023
EFFECTIVE July 5, 2017	DOMAIN Software Security	FAMILY ISO Industry Standards
REGION United States	ADOPTION MODEL Certification	IMPLEMENTATION COMPLEXITY Moderate

Source: https://standardscatalog.ul.com/ProductDetail.aspx?productId=UL2900-1

Why it matters

- **Improve cybersecurity governance** Provide structured requirements to help organizations oversee and coordinate consistent security practices across connected software products.
- **Support regulatory and industry compliance** Enable organizations to demonstrate adherence to relevant regulations and standards through standardized assessment and documentation processes.
- **Enhance product safety and reliability** Reduce vulnerabilities by requiring secure software development and testing practices, leading to safer and more reliable products.
- **Increase audit readiness** Facilitate streamlined internal and external audits by offering clear criteria for security controls in network-connected devices.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports UL 2900-1

Product Security Requirement Library

Structure UL 2900-1 security requirements with mapped controls, owners, and verification tasks.

Security Development Lifecycle Governance

Track security design reviews, coding practices, and lifecycle checkpoints across product development.

Vulnerability and Patch Management for Products

Manage vulnerability findings, remediation tasks, and patch releases affecting connected products.

Security Testing and Verification Evidence

Capture results from penetration tests, code analysis, and product security validation activities.

Supplier and Component Security Oversight

Track third-party software components, supplier security documentation, and dependency risks.

Certification and Compliance Reporting

Provide dashboards summarizing requirement coverage, remediation status, and readiness for UL cybersecurity certification.

Common framework mappings

CIS Controls v8.1 | COBIT 2019 | GDPR | ISO 27001:2022 | ISO 27002:2022 | NIST CSF 2.0 | NIST 800-53 Rev.5 | PCI DSS 4.0.1 | SOC 2

Official resources

UL 2900-1 Standard

Defines general requirements for software cybersecurity in network-connectable products.

ulstandards.ul.com/standard/02900-1_2

UL Cybersecurity Assurance Program

Outlines the certification program for products adhering to UL cybersecurity standards.

ul.com/resources/cybersecurity-assurance-program

UL Product iQ Database

Provides access to certifications related to UL 2900-1 compliance and products.

productiq.ulprospector.com/en

Explore UL Standards

Offers information and documents related to various UL cybersecurity standards.

ulstandards.ul.com/understand-the-process

Frequently asked questions

What is UL 2900-1 used for?

UL 2900-1 specifies general cybersecurity requirements for network-connectable products and systems, ensuring they are designed and maintained to address known cybersecurity risks. It is used by manufacturers and vendors to establish a baseline for software security practices.

Is UL 2900-1 certification required?

UL 2900-1 certification is voluntary unless mandated by a specific industry or regulatory body. Organizations may choose UL 2900-1 certification to demonstrate compliance with recognized cybersecurity standards for their products.

What types of products fall under the scope of UL 2900-1?

UL 2900-1 applies to products and systems that are network-connectable and contain software components, such as IoT devices, medical equipment, and industrial controls. The standard covers both stand-alone products and integrated systems exposed to potential cyber threats.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What key requirements or artifacts are specified in UL 2900-1?

Key requirements include threat modeling, secure software development lifecycle (SDLC) practices, vulnerability testing, patch management processes, and creation of security documentation. Artifacts may include risk assessments, penetration test results, and secure coding reviews.

How do organizations implement UL 2900-1?

Implementation involves conducting cybersecurity risk assessments, adopting secure coding standards, integrating security testing, and maintaining ongoing vulnerability management procedures within the product development process. Documentation of controls and security processes is essential for demonstrating compliance.

How does UL 2900-1 relate to other cybersecurity standards?

UL 2900-1 aligns with widely recognized standards such as ISO/IEC 27001, NIST SP 800-53, and IEC 62443 concerning software and product security. It is often used alongside these frameworks to address the specific cybersecurity needs of embedded and networked software products.

What ongoing compliance activities are required under UL 2900-1?

Organizations must perform ongoing vulnerability assessments, monitor for emerging threats, apply security updates as needed, and maintain documentation of incident responses and remediation efforts. Regular reviews and updates of security controls are necessary to retain compliance.

How would SmartSuite support UL 2900-1?

SmartSuite can help organizations manage UL 2900-1 compliance by centralizing risk tracking, managing controls and remediation activities, and organizing evidence collection for audits. It supports workflow management for security processes, enables audit readiness with tailored checklists, and automates reporting for continuous compliance monitoring.

License included / downloadable: No UL 2900-1 is published by Underwriters Laboratories (UL) and the official standard requires purchase from UL or authorized standards retailers. License not included with platform

Full framework page and mappings: smartsuite.com/frameworks/ul-2900-1-software-cybersecurity-network-connectable-products

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.