Cybersecurity

Empowering product innovation with the UL Cybersecurity Assurance Program (CAP)

The UL Cybersecurity Assurance Program (CAP) is intended to support manufacturers, end-users and system installers & integrators in promoting good cybersecurity hygiene in building, installing and maintaining products and systems. Based on the UL 2900 Series of Standards and other industry standards, the full suite of cybersecurity services is designed to help organizations manage their cybersecurity risks and validate their cybersecurity capabilities to the marketplace.

Advisory Services

Gap Assessment

A workshop with technology teams to assess an organization's products or its process alignment with an industry best practice or standard. The workshop process identifies areas for improvement and compliance, including:

- Scoping of products & systems and their applicable security requirements
- Readiness for potential cybersecurity certification

Training

Customized instructor-led training to fit an organization's cybersecurity educational needs. Support and educate team members on wide-ranging areas including:

- Good design practices
- Threat analysis
- Risk management
- Cybersecurity testing
- Applicable standards and best practices

Secure Development Lifecycle (SDL)

Including cybersecurity into the design, testing and maintenance of an organization's product lifecycle can help promote good cybersecurity in products and systems. UL can support these initiatives through customized support on training, building and assessing an organization's SDL, including:

- Security requirements, program and policy review
- Threat analysis with modeling
- Secure software design
- Coding standards and code analysis
- Risk management
- Penetration testing

Organizational and Process Security Assessment

Including cybersecurity requirements into organizational policies, procedures, and supplier agreements can help promote good cybersecurity throughout an organization and supply chain. UL can support these initiatives through customized support on training, building and assessing an organization's security policies and procedures, including:

- Organizational policy and procedures review
- Supply chain policy review
- Business risk management

UL Cybersecurity Assurance Program (CAP)

Based on the UL 2900 Series of Standards and other industry standards, UL's Cybersecurity Assurance Program (CAP) includes a wide range of service offerings within the following categories:

ADVISORY

TESTING

CERTIFICATION

Testing Services

Penetration Testing & Security Assessments

A structured security assessment based on IoT and cybersecurity standards and best practices, penetration testing involves discovering and exploiting software vulnerabilities with extensive hacking techniques – including embedded systems analysis and firmware evaluation that can be applied to systems from:

- Endpoints
- Devices
- Gateways
- Cloud systems
- Mobile applications

Certification Services

UL 2900 Series of Standards

Certification of a product, component, device or system based on standardized, testable criteria to assess and benchmark software vulnerabilities and weaknesses that can impact the cybersecurity hygiene of a product, component, device or system. This certification provides validation of an organization's cybersecurity due diligence to end customers according to the UL 2900 Series of Standards, including:

- Product Requirements

- 2900-1 – Software
- 2900-2-1 – Healthcare Systems
- 2900-2-2 – Industrial Control Systems
- 2900-2-3 – Building Security Systems
- 2900-2-4 – Building Automation (2019)
- 2900-2-5 – Lighting (2019)

- Process Requirements

- 2900-3-1 – Process Requirements (2019)
- 2900-3-2 – Secure Development (2019)

IEC 62443 Family of Standards

The IEC 62443 family of standards has cybersecurity procurement requirements for an end-user or asset owner to specify for acquisition of industrial automation control systems. Certification to these standards demonstrate to customers that an organization has done the due diligence of building cybersecurity into their processes and practices according to the IEC 62443 family of standards, including:

- 62443-2-4 – Security Practices
- 62443-3-3 – Security Functions
- 62443-4-1 – Secure Development Lifecycle
- 62443-4-2 – Component Security

To learn more about the UL Cybersecurity Assurance Program (CAP), visit UL.com/cybersecurity or email: ULCyber@ul.com

Empowering Trust™

CYB-082918