Managing cybersecurity risk in the supply chain

UL Supplier Cyber Trust Level

Cybersecurity is a major concern that affects manufacturers, suppliers and end product ecosystems.Procurement mechanisms need to be established to help suppliers and vendors better demonstrate the trustworthiness of their security practices. Increased diversity and complexity of global supply chains lead to growing cybersecurity threats. Upholding cybersecurity requirements and strong cooperation with third parties is essential.

Manufacturers, suppliers and end product ecosystems are only as strong as their weakest link and to aid procurement mechanisms and strengthen the overall supply chain, UL is launching the Supplier Cyber Trust Level. The goal of this solution is to help industrial, automotive and medical device organizations minimize risk of introducing security issues into their end products that could expose software or system vulnerabilities for customers and end product use.

Supplier Cyber Trust Level

UL's Supplier Cyber Trust Level helps suppliers and vendors better navigate procurement and quality assurance processes by demonstrating the trustworthiness of their security practices across the following key trust categories:

- Software development practices
- Software development environment and infrastructure
- Hardware development practices
- Product documentation
- Secure production process and delivery management
- Security issue management
- Hosted software
- Quality management system
- Enterprise security
- Supplier management

Suppliers and vendors benefit from a single security level provided through an experienced assessment and evaluation process. The Supplier Cyber Trust Level also helps with an additional level of competitive differentiation via an independent, documented supplier Trust Level rating

Supplier Trust Level Ratings:

- Level 1: Nascent – No or few ad-hoc security practices have been implemented. Need to consider security in all processes related to the products/services provided to customers.
- Level 2: Challenger – Basic security practices have been incorporated in some processes. Need to consider security in all processes related to the products/services provided to customers.
- Level 3: Contender – Intermediate security practices have been incorporated in some processes. Need to consider security in all processes related to the products/services provided to customers.
- Level 4: Strong Performer – Advanced security practices have been incorporated in most of the processes. With some process improvements it is possible to reach the highest trust level.
- Level 5: Leader – Highest trust level attained. Security practices have been incorporated in all trust categories at the expected level.

As an independent trusted third party, UL helps manage the Supplier Cyber Trust Level on behalf of organizations as a time-efficient and cost-efficient process to assess supply chain security risk.

UL's Supplier Cyber Trust Level helps navigate the current global complexity of cybersecurity by mapping and leveraging security controls from well-known/popular industry best practices, standards and frameworks, including:

- NIST cyber supply chain risk management
- ENISA supply chain attacks
- METI Society 5.0
- NERC CIP-013-1UK Supplier Assurance
- ISO/IEC 20243-1
- IEC 62443-4-1 & 62443-2-4
- ISO 27001
- NERC

Key solution objectives

Understanding cybersecurity risks within the supply chain:

- Leveraging procurement mechanisms to incorporate cybersecurity risk management in the supply chain
- Addressing secure development lifecycle (SDL) criteria with industry-accepted standards, framework and best practices
- Demonstrating the trustworthiness of supplier and vendor security practices

Questions and practices assessed for IoT suppliers and vendors

UL's Supplier Cyber Trust Level provides in-depth analysis across 10 trust categories to assess supplier and vendor practices such as:

- Do they have adequate safeguards in place to minimize cybersecurity risk associated with information security and development, deployment and use of software/hardware products or components, with regular follow-ups?
- Do they leverage organizational cybersecurity criteria and requirements, including standard and framework requirements, for all in-house developed and third-party software/hardware products and components?
- Do they ensure sufficient protection against security flaws and weaknesses for all software/hardware?
- Do they identify potential software vulnerabilities that may result in a compromise on a regular basis?
- Do they perform ongoing evaluation and validation of software/hardware products and components for compliance with organizational cybersecurity criteria and requirements?
- Do they have a formal process for identifying potential software vulnerabilities and updating software and applying patch updates as appropriate to ensure ongoing protection against new security threats and risks?
- Do they leverage independent third party evaluation to validate security of in-house developed and third-party software/hardware?

UL benefits for IoT supply chains

We are a recognized leader in security advisory, testing, audit and certification services in markets regulated for security, such as payments and federal procurement.
We offer a growing list of IoT security solutions, including UL's IoT Secruity Rating, UL Cybersecurity Assurance Program (CAP), IEC 62443 and other training and advisory services that address secure product development, cybersecurity in smart ecosystems and supply chain risk management.

Unlike many security firms that mainly have IT and risk management backgrounds, UL has many years of experience performing security evaluations of both hardware and software-based products and assessments of their development practices per industry best practices.

With the Supplier Cyber Trust Level, UL helps:

- Address and reduce the security risks associated with IoT supply chains
- Support industry and stakeholder collaboration to promote sharing of cybersecurity lessons learned and best practices
- Develop and utilize appropriate metrics and evaluation methods for cybersecurity assurance of IoT supply chains
  Support organization procurement needs to help suppliers and vendors better demonstrate the trustworthiness of their security practices
- Provide external cybersecurity expertise and organizational bandwidth support

For more information on UL's Supplier Cyber Trust Level, email us at imsecurity@UL.com or visit ims.UL.com/Supplier-Cyber-Trust-Level.

Empowering Trust®