EU Cyber Resilience Act (CRA) Recommended Supplier Requirements

The European Union's Cyber Resilience Act (Regulation (EU) 2024/2847) introduces mandatory cybersecurity requirements for virtually all products with digital elements sold in the EU market, with full enforcement beginning December 11, 2027.

Applied Materials is committed to ensuring that our products and those of our suppliers meet the requirements of the CRA.

This document outlines what the CRA requires and what Applied Materials needs from you as a supplier.

Version 1.0 — September 2026. This document is provided for information only. It summarizes Applied Materials' expectations of its suppliers under Regulation (EU) 2024/2847 and does not constitute legal advice. It does not amend or replace the terms of any purchase order or supplier agreement between you and Applied Materials; where this document and that agreement differ, the agreement controls.

What is the Cyber Resilience Act?

The Cyber Resilience Act is the EU's first horizontal regulation establishing uniform cybersecurity requirements for hardware and software products placed on the European market. It aims to improve cybersecurity across the EU by imposing mandatory requirements on “products with digital elements”.

The CRA's reach is global. The regulation focuses not on where a product is manufactured but on whether it is made available on the EU market. Any manufacturer wishing to sell a product in the EU must comply, regardless of where it is headquartered or where production occurs.

Two dates, two phases — and what each means for you

The CRA arrives in two stages, and each affects you differently.

Phase 1 — Reporting, from September 11, 2026. From this date Applied must report actively exploited vulnerabilities and severe incidents in its products to EU authorities on tight clocks (see Reporting Requirements below). Applied cannot meet those clocks unless you tell us quickly when a vulnerability or incident affects a component you supply. This phase is about communication channels and speed, not certification.

Phase 2 — Full compliance, from December 11, 2027. From this date every product with digital elements Applied places on the EU market must meet the CRA's essential cybersecurity

requirements, carry CE marking, and be backed by technical documentation, an SBOM, a vulnerability-handling process, and security updates for a defined support period. Applied assembles these from the evidence you provide for your components.

Existing and legacy products. The CRA applies to products that continue to be placed on the EU market after December 11, 2027 — not only brand-new ones. If a component you supply goes into an Applied product that keeps being sold (or is substantially modified) after that date, it is in scope, and we will need the same evidence and support from you for it. Products already in the field that are not placed on the market again are treated differently.

Reporting Requirements

Due: September 11, 2026

Scope: If the supplied component is in scope for EU CRA and is destined to be placed on the market by Applied Materials, then the supplier is responsible for the following requirements. Applied determines whether a given product sold to Applied is in scope for the EU CRA and intended for the EU market. Applied will confirm scope determinations, and any later change to them, in writing through the supplier's Applied procurement contact; obligations for a newly in-scope component begin on that notice, with a reasonable period to implement. If a supplier separately places the same component sold to Applied on the EU market as its own product, the supplier is independently responsible for that placement's EU CRA compliance and must notify Applied of it in writing through its Applied procurement contact within 30 days of placement, identifying the product, the conformity-assessment route used, and the DoC reference. A new notification is required for any variant or firmware version placed under a separate declaration of conformity.

Why these timelines matter to Applied. From September 11, 2026, when Applied becomes aware of an actively exploited vulnerability or a severe incident in one of its products, Applied must file an early warning to EU authorities within 24 hours, a fuller notification within 72 hours, and a final report within 14 days of a corrective measure becoming available. Applied's clock starts when Applied becomes aware. When an issue originates in a component you supply, notify Applied early enough for us to meet these deadlines — tell us what you know immediately and update us as facts develop. Reciprocally, where Applied first observes an actively exploited vulnerability or severe incident in a deployed Applied system that is reasonably attributable to a supplied component, Applied will notify the supplier without undue delay — subject to Applied's legal, confidentiality, and customer obligations — so the supplier can assess cross-customer impact and meet its own CRA obligations.

General Reporting Requirements

1. Suppliers shall have a vulnerability and incident reporting process that is operational — documented, staffed by named personnel or a monitored intake address, and exercised at least annually — and shall provide evidence of each on Applied's request.
2. Suppliers shall have a single point of contact for communication related to cybersecurity. Notifications under these requirements shall be sent without undue delay by calling or emailing the Supplier Account Manager (SAM) and by email to AMAT_Supplier_Cybersecurity@amat.com. Where a notification contains sensitive vulnerability or incident detail, use the encryption keys Applied provides for that purpose.
3. Suppliers shall notify Applied of any actively exploited vulnerability or severe incident affecting a supplied component within 24 hours of becoming aware independently of Applied, and in any event without undue delay, so that Applied can meet its own CRA reporting deadlines. This contractual notification is in addition to, and does not substitute for, any independent reporting obligation the supplier owes to EU authorities under Article 14.
4. Supplier shall work collaboratively with Applied regarding the vulnerability or incident until resolution — meaning a fix, mitigation, or accepted compensating control is in place and both parties confirm closure in writing. Each party shall name an escalation contact, and severity shall be classified jointly using CVSS or another agreed method.
5. Each notification and update under these requirements shall be labeled with its sensitivity classification (for example, public, confidential, or restricted) and sent through the secure channel Applied designates for cybersecurity notifications.

Actively Exploited Vulnerability Requirements

1. For actively exploited vulnerabilities — whether in the supplier's own code or in any third-party or open-source component integrated into the supplied component — the supplier shall provide the following to Applied Materials within the notification timeline in General Reporting Requirement 3, with facts not yet available supplied as they develop:
    - Description of the vulnerability, including known identifiers (e.g., CVE, EUVD) if assigned.
    - Affected component name, version(s), and configuration(s) supplied to Applied.
    - Exploitation status, including whether exploitation has been confirmed, observed in the wild, or reported by a trusted third party, and the supplier's assessment of whether the vulnerability is reachable and exploitable in the configuration supplied to Applied. A supplier assessment of non-exploitability does not relieve the supplier of the obligation to notify; Applied makes the final determination for its integrated product.

- Known or potential impact of exploitation on the confidentiality, integrity, or availability of the component or the data it processes, including any effect on essential functionality.
- Available mitigations, workarounds, or fixes, and the expected remediation timeline. If no remediation is planned, or the decision has not yet been made, the supplier shall state that expressly, with the reason and any available workaround or compensating control.
- Updates without undue delay on any of the following: a change in exploitation status (for example, a proof of concept published or exploitation confirmed in the wild); identification of additional affected versions or configurations; a change in remediation status; or a material change in the severity assessment.

Severe Incidents Requirements

1. For severe incidents the supplier shall provide the following to Applied Materials:
   - Description of the incident, including what is known at the time of notification.
   - Affected component name, version(s), and configuration(s) supplied to Applied.
   - Nature of the impact or potential impact, including effects on the confidentiality, integrity, or availability of the component or the data it processes, and any effects on safety-related behavior, or essential functionality.
   - Technical scope: affected component versions, hardware revisions, firmware versions, and configurations.
   - Deployment scope, if known: the number of units supplied to Applied that are affected.
   - Known or suspected cause of the incident (if identified).
   - Mitigation or containment actions taken or planned, including status expressed as one of: planned, in progress, deployed, or not planned (with reason).
   - Updates without undue delay on any change in the incident's status, scope, cause, or remediation plan, and in any event on closure.
   - After the incident is closed:
     - A detailed description of the incident, including its severity and impact.
     - The type of threat or root cause that is likely to have triggered the incident.
     - Mitigation measures applied and ongoing.

Essential Cybersecurity Requirements

Due: December 11, 2027

Scope: If the supplied component is in scope for EU CRA and is destined to be placed on the market by Applied Materials, then the supplier is responsible for the following requirements (see Scope under Reporting Requirements above for how scope is determined).

A. **Risk-based design:** Components must be designed, developed and produced to ensure an appropriate level of cybersecurity based on the risks, informed by a documented cybersecurity risk assessment.

B. **Secure by Design (EU CRA Annex I Part I)**
   a) No known exploitable vulnerabilities at the time the component is placed on the market.
   b) Secure-by-default configuration, including the ability to reset to the original secure state.
   c) Security updates mechanism: vulnerabilities must be addressable via updates; where applicable, automatic updates on by default, with user notification, easy opt-out, and ability to postpone.
   d) Protection from unauthorized access via authentication, identity/access management, and reporting of access attempts.
   e) Confidentiality of stored, transmitted, and processed data using state-of-the-art encryption at rest and in transit.
   f) Integrity of data, commands, programs, and configuration: protection against unauthorized modification, with corruption reporting.
   g) Data minimization — only process data adequate, relevant, and limited to the intended purpose.
   h) Availability of essential/basic functions, including resilience and DoS mitigation, even after an incident.
   i) Minimize negative impact on other devices/networks (no degradation of services provided by other systems).
   j) Limit attack surfaces, including external interfaces, by design.
   k) Reduce incident impact through appropriate exploitation mitigation techniques (e.g., sandboxing, ASLR, privilege separation).
   l) Security monitoring & logging: record and monitor access to/modification of data, services, and functions, with a user opt-out.
   m) Secure data deletion / transfer: users must be able to securely and permanently remove all data and settings, and any transfer to another system must be done securely.

C. **Vulnerability Handling (Annex I Part II)**

a) Identify and document vulnerabilities and components, including an SBOM in a machine-readable format covering at least the top-level dependencies of the component (EU CRA Annex I Part II(1)). Top-level coverage is Applied's minimum; where your build tooling produces deeper transitive data, provide it, and Applied may request transitive coverage for higher-risk components. For Applied specifically: provide a current SBOM for each supplied component in a machine-readable format — CycloneDX and SPDX are both acceptable, and Applied has not mandated a single format, delivered with each release and refreshed whenever the component's composition changes. Applied relies on your SBOMs to build the SBOM the CRA requires in its own technical documentation, so completeness and timeliness are essential.
b) Address and remediate vulnerabilities without delay, providing security updates separately from functionality updates where feasible.
c) Apply effective and regular security tests and reviews of the product.
d) Publicly disclose information on fixed vulnerabilities once a security update is available, including description, affected product, impact, severity, and remediation guidance.
e) Establish and enforce a coordinated vulnerability disclosure (CVD) policy.
f) Facilitate sharing of information on potential vulnerabilities in the product and its third-party components, including a contact address for reporting.
g) Provide mechanisms to securely distribute updates, automatically where applicable.
h) Disseminate security updates without delay, free of charge, with advisory messages on actions users should take.
i) Provide security updates and support for each supplied component throughout the support period Applied declares for its product — its expected product lifetime, as communicated by Applied for that product. The CRA requires Applied to declare and honor a support period, and Applied can only commit to it if you commit to support your components for the same period. Applied will communicate the declared support period for each affected product in writing through procurement documentation at or before award, and will notify you of any change to it. Tell Applied promptly — and in any event at least 12 months before the date concerned — if you plan to end support for a supplied component.

D. Technical Documentation

a) Prepare and maintain CRA-compliant technical documentation for the supplied component, covering all elements of Annex VII (general description, risk assessment, SBOM, vulnerability handling processes, test reports, support period justification, standards applied, DoC).
b) Retain the documentation for at least 10 years after the component is placed on the market or for the support period, whichever is longer.

c) Keep the documentation current throughout the support period — update it whenever the component changes, vulnerabilities are remediated, or risk assessments are revised.
d) Provide a written attestation to Applied confirming that complete Annex VII technical documentation exists, is maintained, and is available on request.
e) Make the documentation available to Applied on reasoned request when needed to support Applied's own conformity assessment, risk assessment, incident investigation, or response to a market surveillance authority.
f) Share the following extracts proactively — Applied needs them to build its own Annex VII technical documentation and cannot assemble that on a request-and-wait cycle — while retaining the full file internally. Provide them at first delivery and refresh them whenever the underlying content changes:
    - SBOM (machine-readable, e.g., CycloneDX or SPDX).
    - Cybersecurity risk assessment summary.
    - Vulnerability handling process description (PSIRT/CVD policy).
    - Support period declaration and justification.
    - List of harmonized standards / certifications applied (if any).
    - EU Declaration of Conformity (once CE-marked).
g) Cooperate with market surveillance authorities directly if requested, and notify Applied promptly, to the extent legally permitted, of any such request or investigation affecting the supplied component. Applied is the manufacturer of record for the integrated product and may face parallel inquiries or corrective-action obligations, so it cannot respond effectively without notice.
h) Ensure, by contract or other effective means, that the supplier can obtain from its own sub-suppliers — and for open-source dependencies — the information needed to meet the obligations in this section, and can provide that information to Applied. Applied does not prescribe the form of the supplier's sub-tier arrangements, only that the information flow be available.
i) Support Applied's supply-chain due diligence. Article 13(5) of the CRA requires Applied to exercise due diligence over the components it integrates, including free and open-source components, so that those components do not compromise the cybersecurity of Applied's product. Article 13(6) further requires Applied, on identifying a vulnerability in an integrated component — including an open-source component — to report it to the person or entity manufacturing or maintaining that component and to remediate it in accordance with Annex I Part II; Applied cannot do either without knowing what is in the component and its current vulnerability status. On Applied's request, provide component provenance at the level of the third-party and open-source components identified in the SBOM (Applied does not require commercial terms or pricing relating to your sub-tier suppliers), the current known-vulnerability status of the component (open CVE/EUVD entries and their remediation status), and confirmation that you monitor the component and its dependencies for newly disclosed vulnerabilities.

j) Notify Applied of any change to the technical documentation that could affect the compliance of Applied's integrated product (i.e., its cybersecurity posture), including changes in support period, SBOM composition, or risk profile.

E. Conformity Assessment and CE Marking

a) **Conformity Assessment:** Carry out the applicable conformity assessment procedure under Article 32 of the EU CRA (internal control, EU-type examination, or full quality assurance) appropriate to the product category (default, important Class I/II, or critical). Notify Applied if you classify your component as anything other than 'default,' since that can affect Applied's conformity-assessment route and product classification.

b) **EU Declaration of Conformity (DoC)**: Draw up a written EU Declaration of Conformity in accordance with Article 28 and Annex V of the EU CRA, declaring that the essential cybersecurity requirements in Annex I have been fulfilled.

c) **DoC Content:** Ensure the DoC includes at minimum:
- Product name, type, batch/serial number, and unique identifier.
- Supplier's name and address.
- Statement that the DoC is issued under the sole responsibility of the supplier.
- Reference to Regulation (EU) 2024/2847 and any other applicable Union legislation.
- References to harmonized standards, common specifications, or European cybersecurity certification schemes applied.
- Place and date of issue, signature, name, and function of the signatory.

d) **CE Marking:** Where applicable, affix the CE marking visibly, legibly, and indelibly to the product in accordance with Articles 29 and 30 of the EU CRA, and to its packaging and accompanying documentation.

e) **Language and Format:** Provide the DoC in a language easily understood by users and market surveillance authorities in the Member States where the product is made available, and supply it in both printed and machine-readable electronic formats.

f) **Retention:** Retain the EU Declaration of Conformity and supporting technical documentation for at least 10 years after the product is placed on the market and make them available to Applied Materials and to market surveillance authorities upon reasoned request.

g) **Updates and Re-issuance:** Update and re-issue the DoC whenever changes to the product, its components, vulnerability handling processes, or applicable standards affect conformity.

h) **Notification of Non-Conformity:** Notify Applied Materials in writing within 48 hours of becoming aware that the supplied product no longer conforms to the EU CRA essential requirements or that the attestation, DoC, or CE marking is no longer valid.

i) **Sub-Supplier Flow-Down:** Require any sub-suppliers of integrated digital components to provide equivalent CE marking and EU Declaration of Conformity, or

where not directly required, equivalent attestations of compliance with Annex I, Part I and Part II.

j) **Provision to Manufacturer:** Deliver a copy of the current EU Declaration of Conformity to Applied Materials at first delivery, on each product release or version change affecting conformity, and on Applied's request at any time, in each case prior to integration into Applied Materials' products. A per-shipment copy is not required where the DoC already on file remains current.

Resources

Official CRA Legislation and EU Guidance

- Full text of Regulation (EU) 2024/2847 (Cyber Resilience Act)
- European Commission CRA Summary
- European Commission CRA Implementation Page
- CRA Reporting Obligations and Single Reporting Platform
- CRA Standardisation Page
- European Commission CRA Implementation FAQ (December 2025)
- Implementing Regulation (EU) 2025/2392 (Product Category Technical Descriptions)

Standards and Frameworks

- STAN4CRA.eu: Joint CEN/CENELEC/ETSI standards development portal for CRA harmonised standards
- CEN-CENELEC M/606 Work Programme (PDF): Full list of 41 harmonised standards under development, with assigned committees and expected publication dates
- ETSI CRA Draft Standards (Public Consultation): Access draft European Standards for comment
- ENISA: CRA Implementation via EUCC: Analysis of how EU cybersecurity certification supports CRA conformity
- European Vulnerability Database (EUVD): Centralized EU vulnerability information platform
- NANDO Database (Notified Bodies): Locate designated conformity assessment bodies

Contact

For general inquiries about Applied Materials' cybersecurity requirements for suppliers, contact your Applied Materials procurement representative. For CRA cybersecurity notifications and questions, contact your Supplier Account Manager (SAM) and email

AMAT_Supplier_Cybersecurity@amat.com. We encourage suppliers to begin their CRA readiness assessments now and to reach out with questions early in the process.

Next steps for suppliers

1. Confirm with your Applied contact whether the components you supply are in scope and destined for the EU market.
2. Share your single cybersecurity point of contact and confirm how you will send and receive notifications.
3. Assess your SBOM, vulnerability-handling, and conformity-evidence capabilities against the requirements above, and raise any gaps with Applied early.
4. Review the CRA terms in Attachment 23 to your Applied supplier agreement.
5. Note that where an Applied purchase order or supplier agreement requires CE marking on a component, CRA conformity obligations follow from that requirement independently of Applied's EU-market scope determination. Raise any apparent inconsistency between a CE-marking requirement and a scope determination with your Applied contact.
6. Engage Applied early on CRA-driven component changes — firmware updates, configuration changes, or new security features — which may trigger Applied's change-control and re-qualification process. Plan change windows so that re-qualification completes before the applicable CRA deadline.