CONFIDENTIAL COMPUTING CONSORTIUM

Governance Risk & Compliance Special Interest Group

Expectations of Ecosystem Participants

August 2025

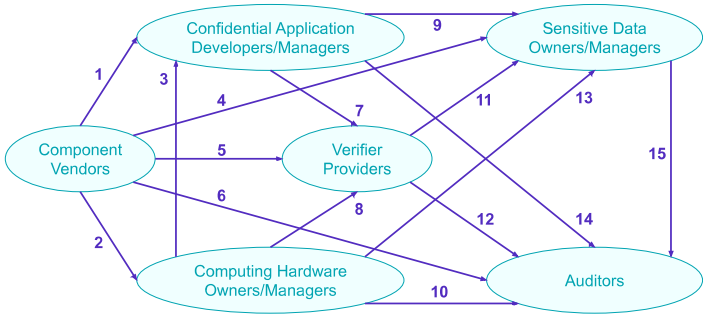
Context

In any environment employing Confidential Computing, there are several distinct classes of participants, and their relationships are generally the same across all such environments.

Problem

This pattern sets out to list in one place the high-level requirements that various participants in the Confidential Computing ecosystem are likely to place on each other from the governance perspective.

Solution



The table below contains the generalized summaries of expectations across each of the numbered relationships in the diagram above. Individual Governance Patterns describe these expectations in extensive detail.

#	Description
1, 2, 4, 5	The **Component Vendors** are responsible for: • Publishing patches and their associated Reference Values/measurements • Addressing discovered vulnerabilities in a responsible and timely fashion • Ensuring their offerings are compatible with appropriate standards, protocols, and regulations • Demonstrating trustworthiness and continuously improving the soundness of their offerings through sustained security efforts involving state-of-the-art scientific methods and third-party security reviews • Operating the manufacturing process behind their products in accordance with appropriate regulations and certification requirements
3,13	**Computing Hardware Owners/Managers** are responsible to the **Confidential Application Developers/Managers** and **Confidential Data Owners/Managers** for: • Timely deployment of patches supplied by the **Component Vendors** • Operating the hardware in their possession in accordance with relevant specifications from the Component Vendors (e.g., ensuring physical security, secure configuration, etc.) • Secure decommissioning of the hardware in keeping with the **Component Vendors'** recommendations
6, 10, 12, 14, 15	All parties may be required to provide evidence in support of satisfying the regulatory and contractual obligations listed in various Control Specifications to the **Auditors**.
7	The **Confidential Application Developers/Managers** are responsible to the **Verifier Providers** for supplying the up-to-date measurements of code and configuration that would subsequently be deployed to perform confidential computations.
8	**Computing Hardware Owners/Managers** are responsible to the **Verifier Providers** for: Timely coordination and deployment of hardware patches following their publication by the Component Vendors
9	The **Confidential Application Developers/Managers** are responsible to the **Confidential Data Owners/Managers** for: • Development of Confidential Applications in keeping with appropriate current best practices • Secure deployment of the Confidential Applications • Timely notification of breaches, discovered security vulnerabilities in their Confidential Applications, and other security incidents • Timely development and deployment of patches for functionality defects and security vulnerabilities
11	The **Verifier Providers** are responsible to the **Confidential Application Developers/Managers** for: • Operating their offerings in a highly available fashion • Ensuring peer isolation in situations involving multi-tenancy • Timely incorporation of patches and other recommendations, such as secure configuration, from the **Component Vendors** • Complying with legal disclosure obligations regarding breaches and other security incidents • Collecting and securely storing all logs and evidence related to service operation, histories of policies and changes, etc.