CCC Governance Risk & Compliance Special Interest Group – Charter

Governance – Definition

Govern (*tr. v.*): To control, direct, or strongly influence the actions and conduct of

Background

Every time a new security technology with broad applicability emerges, regulations follow. This usually happens after the technology in question is deployed beyond some critical mass: in other words, regulations do not go into effect until there is a way for regulated entities to comply with them. This has already happened with data-in-transit and data-at-rest protections. Confidential Computing will shield data-in-use, completing the trifecta.

Regulatory bodies vary in scope: regulations are put in place by nation states (Luxembourg), federal agencies (SEC), state legislatures (California), industry bodies (PCI-DSS), and regional powers (GDPR). Regardless of scope, all regulators demand that the subjects of regulations achieve, maintain, and prove on demand compliance with a given set of criteria. Failure to comply can be very costly indeed: for instance, a financial firm may lose its license to operate, effectively putting it out of business. As a result, regulated institutions treat these matters extremely seriously. In addition, even outside of externally imposed regulations, a business may enter into contractual relationships with its customers and/or suppliers, and then would also need to assess compliance with those commitments.

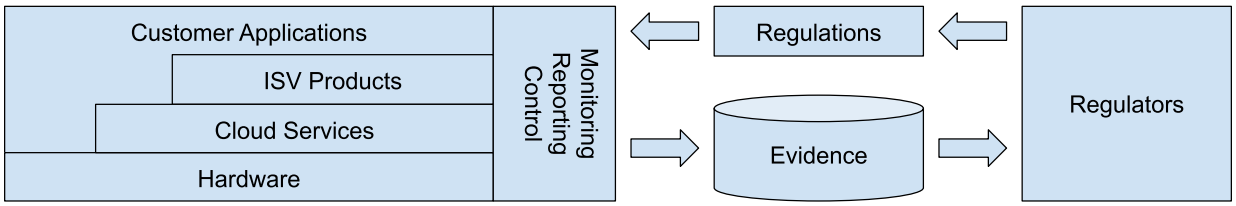
Governance-related activities comprise the following main components:

1. Articulating the desired state of a system[1] (or, alternatively, forbidden states), as well as specifying the actions to be taken when a breach is detected; as regulations and/or contractual obligations change, these are subject to change as well
2. Measuring the state of the system (through continuous monitoring, sampling and/or periodic reviews)
3. Comparing the reported state of the system against the desired state
4. When an undesirable state or condition is detected, taking prescribed actions to bring the system back into compliance
5. Testing effectiveness by periodically triggering undesirable states and ensuring that the system responds in the expected way (e.g., self-correcting violations or terminating offending workloads)

[1] "State of a system" necessarily comprises attributes of the data being processed, as well as attributes of the IT systems doing the processing.

6. In all steps above, documenting (“evidencing”) all pertinent information and storing the evidence for a period of time required by the regulators
7. Presenting the evidence from the previous steps to regulators, periodically and/or on-demand

There is often only a partial overlap between security and compliance requirements, resulting in outcomes where a system can be very compliant and not very secure, or vice versa. Given the certainty of a review by oversight bodies, versus only a chance of being attacked by an adversary, regulated institutions will almost always prioritize compliance over security. Therefore, well-articulated compliance requirements that take security into account, are more likely to result in better security outcomes as well.



Picture 1: High-level governance architecture for Confidential Computing

Goals

The goals of the CCC Governance SIG fall into two main categories, outlined in the following subsections.

1. Support for the Creation of Effective Regulatory Frameworks

The CCC Governance SIG will partner with regulators in crafting governance frameworks for Confidential Computing that also:

- Align with the desire of regulated customers, as well as consumers of data processing devices and services, to better safeguard their data while in use – better compliance should also mean better overall security outcomes!
- Support the desire of data processors and consumers and consumers to reduce business and reputational risks of breaches, operator errors, and/or surveillance the world over, that could otherwise lead to exfiltration or tampering of customer data
- Provide relevant and actionable guidance to independent solution vendors
- Confidential Computing being a hardware-assisted technology at its core, guide hardware vendors in providing the necessary foundations for all of the above
- Support creation of actionable guidance for assessors and auditors for evaluating compliance of confidential computing systems with corresponding regulations

2. Recommendations for Repeatable Patterns and Tooling

As any regulated customer with large application and device fleets knows, the key to governance and compliance at scale is repeatability. Therefore, additionally and separately, we will support creation of reusable software patterns around attestation, deployment, updating, monitoring, evidencing, assessment, and control of confidential computing solutions that would help inform cloud providers and independent solution vendors, and that can be easily adopted by the developers of the next generation of Confidential Computing-native applications.

We will seek to achieve these goals by bringing together influential and knowledgeable representatives from the following five constituencies:

1. Silicon vendors
2. Public cloud providers
3. Independent solution vendors
4. Regulated industries
5. Regulatory bodies