Damage Assessment

IPC-1792 recommends that when a suspected cybersecurity incident occurs, the criteria for determining the event as an incident be prepared in advance. Based on these criteria, it is decided whether to transmit the incident to other stakeholders the supply chain.

It is essential that this judgement criteria be based on facts.

As an example of a judgment flow, when a stakeholder (factory) identifies a cybersecurity incident, it must conduct a damage assessment to determine whether the incident affected the functionality or quality of certified products or materials that are either still within the factory or were shipped during the period the incident. IPC-1792 refers to this as the CIQA. It should be noted that the CIQA is primarily concerned with identifying materials and products that have been compromised or otherwise affected (not relying on any forensic or root cause analysis).

The diagram below is customized and written according to the business of the supply chain entity (factory). It is desirable to be prepared for immediate reference in case of emergency.