| Eclipse Foundation | 332 | 5.5 |  | ge | There are no requirements on open source maintainers nor on open source software stewards to engage in consultations with their users. Open source projects might provide information that helps integrators exercise due diligence, and there even might be a security attestation program in the future facilitating this further, but that is the extent of the information integrators should expect. Clause 5.5 needs to reflect this reality and cannot assume a two-way consultation between open source projects and the integrators. | Be upfront that neither open source maintainers nor open source software stewards are relevant stakeholders in this consultation process, and that when integrating open source components integrators must rely on other stakeholders to carry out this assessment.  Alternatively, exempt open source components from this process altogether or define a specific process for the integration of open source components.  Additionally, note that when integrating open source components, integrators might need to carry out this assessment throughout the component's dependency tree, as they cannot rely on a supplier for having carried out this due diligence for them. |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Eclipse Foundation | 1097 | 6.12.2 |  | te | Not all of the documents outlined in 5.5.4 are relevant (or even possible to obtain) for open source components. | This paragraph should be updated to reflect the expected output of 5.5.4 for open source components. |  |
| Eclipse Foundation | 1101 | 6.12.3 |  | te | Open source components might not state their intended purpose. | Limit the requirement to fitness for purpose. |  |
| Eclipse Foundation | 1104 | 6.12.3 |  | te | It might be entirely feasible to assess that a component meets risk-based requirements without having to assess the process used to arrive at that result. This is particularly true for open source components whose code is open and easily auditable by the manufacturer. | Assessing that third-party components ~~has been designed, developed and produced in such a way that they~~ ensure an appropriate level of cybersecurity based on the risks. |  |
| Eclipse Foundation | 1106 | 6.12.3 |  | ge | Unclear what part of clause 5 this requirement implies. | Please be more specific about what part of the risk assessment this clause is referring to. |  |
| Eclipse Foundation | 1108 | 6.12.3 |  | ge | Open source components do not have a supplier. Make sure that this doesn’t exclude properly documented open source components. | Integrating the component according to the instructions of the component~~s~~ ~~supplier~~ and treating integration related risks; |  |
| Eclipse Foundation | 1111 | 6.12.3 |  | ge | Open source components do not have a supplier. Make sure that this doesn’t exclude properly documented open source components. | Providing measures for maintaining the components cybersecurity based on the instructions of the component~~s supplier~~, e.g. vulnerability handling and incident management. |  |
| Eclipse Foundation | 1116 | 6.12.3 |  | te | Clarify that implementing controls also apply to open source components and that relevant industry best practices should be used in that case (as these might differ from closed source components). | Implementing appropriate cybersecurity controls, based on the risk and considering, but not limited to integrity, confidentiality, authentication, encryption and traceability based on relevant industry best practices for third-party components including commercial, free and open-source components and services used in the product. |  |
| Eclipse Foundation | 1117 | 6.12.3 |  | te | Open source components don’t necessarily provide end-of-life information. | Account for lack of information on EOL in open source components. |  |
| Eclipse Foundation | 1122 | 6.12.3 |  | ge | Requirement is ambiguous about whether the audits should target the manufacturer’s product itself or every single component and their dependencies individually. Clarify that the audits are focused on the product itself. | Ensuring audit activities of the product with digital elements and procedures to address cybersecurity risks of third-party components and services. |  |
| Eclipse Foundation | 1125 | 6.12.3 |  | te | Clarify what kind of monitoring is expected. |  |  |
| Eclipse Foundation | 1125 | 6.12.3 |  | te | Manufacturers routinely include thousands of open source components in their products, the large majority of which do not provide lifecycle information. This requirement would not be reasonably fulfillable. Suggest adapting to industry best practices once the nature of the requirement is clarified per previous comment. | Clarify requirements and adapt it to industry best practices for integrating open source components. |  |