

NIS2 Supply Chain operates with three levels of proportionate cybersecurity. Organisations implement only the level that matches their risk profile and role within the chain.

NIS2-SC10 represents the basic level of cyber hygiene for all companies. It is sufficient for the majority of SMEs. NIS2-SC20 and NIS2-SC30 are intended for IT, OT and critical suppliers, as well as larger and more complex organisations.

## When which level?

NIS2-SC10 (most chosen)	NIS2-SC20 recommended for	NIS2-SC30 recommended for
<ul style="list-style-type: none"> <li>SME suppliers</li> <li>Production, trade, services</li> <li>Limited digital chain impact</li> </ul>	<ul style="list-style-type: none"> <li>IT services</li> <li>OT companies</li> <li>IoT companies</li> <li>Access to customer networks</li> <li>Processing sensitive data</li> <li>Larger companies</li> </ul>	<ul style="list-style-type: none"> <li>Software vendors</li> <li>MSPs / hosting / cloud</li> <li>OT environments for critical systems</li> <li>IT environments for critical systems</li> <li>Large and complex organisations</li> </ul>

NIS2	SC10 BASIC	SC20 SUBSTANTIAL	SC30 HIGH
Complexity	Low	Resourse	High
Implementation time	Short	Average	Extensive
Governance	Basic	Formal	Fully integrated
Supplier risk	Basic	Average	High
Technical depth	Foundation	Deepened	Advanced
OT Measures	-	✓✓	✓✓✓
Software security	✓	✓✓	✓✓✓
Number of measures	17	29	55

## Core principle

NIS2 Supply Chain Certification does not require maximum security for everyone, but appropriate and proportionate cybersecurity for each risk in the supply chain.