IOT SECURITY
SELF ASSESSMENT CHECKLIST

	QUESTION	ANSWER 1	ANSWER 2	ANSWER 3
1 **UNDERSTAND THE CYBERSECURITY MATURITY OF YOUR ORGANISATION AND YOUR ECOSYSTEM**	Do you have a cybersecurity governance in your organization (technological watch, Design, maintenance, incident management, training, legal, contractual, ...)?	Yes, internal	Yes, subcontracted	No
	How would you qualify the cybersecurity maturity of your organisation ?	We have a cybersecurity governance that includes Strategy, measurement, improvement	We have a Operational Process and documentation	We have identified people in charge (internal) or exrternal
	Who are your customers ?	Type : B2C, B2B, B2G	Sectors : Transportation, Energy; industrial ; Health ; Smart cities, ...	I don't know about the end-usage
	Does your customer require a risk analysis, filling a security checklist, a certificate ?	Yes, a certificate	Yes, a risk analysis	Filling a security checklist,
	Are you familiar with Risk analysis ?	Yes - I have already done some	I have already red some	Not really
	Are you familiar with Certification and associated ecosystem (Lab, CB, audit lab) ?	Yes - I have already done some with third party	Yes - I am aware of the certification process	No
	Are you aware of certification schemes that would be applicable to your product ?	Yes, I have selected one	Yes - I am aware of the certification process	Not really
	What kind of assemment are you looking for ?	Certification	Review by a third party	self assessment
	Is there (inter-)national, sectorial regulations applicable to your products rergarding security aspects ?	Yes	No	I don't know
	Do you have a clear view of the distribution of responsibilities if a pb occurs when your product is in the field?	Yes	No	I don't know
	Do you have contractual obligations in terms of security with your customer ?	Yes	No	I don't know
	Do you have contractual obligations in terms of security with your suppliers ?	Yes	No	I don't know
	Do you have a description of the expected usage ?	Yes	No	I don't know
	Do you follow security requirements (Protection Profile, standardised Security requiments, ...) ?	Yes	No	I don't know
	Which level of security are you targeting ?	High (Correctness and robustness)	Subtantial (fonctionnal security)	Basic (documented) / Multiple
	What are the kinds of attack that you are considering ?	High (Correctness and robustness)	Remote	I don't know
	What is the approximate life time of your product in the field ?	5-10 Years	2 to 5 years	less than 2 years
2 **UNDERSTAND YOUR DESIGN AND IMPLEMENTATION STATUS**	Are you using COTS; Open sources	Yes	No	I don't know
	Can you update your product (if yes : expected frequency)	Yes SW update & OTA is part of our strategy	Yes but we have not included that in our roadmap	No
	Do you use/implement Cryptographic algorithms ?	Standardized and following guidances	Proprietary	I don't know
	What kind of development life cycle are you using ? When Security is integrated ?			
	Who takes care of the configuration aspects ?	Assigned to a dedicated resource	Shared among the organization	I don't know
	Do you follow coding guidelines ?	Yes	No	I don't know
	Do you have a description of your security architecture ?	Existing and reviewed	To be reviewed ad/or completed	Do be developed
	"Is your product documented ?	Existing and reviewed documentation	Documentation to be reviewed/updated/completed	Documentation to be developed
	How automated is your deployment process ?	CD	Only CI	None
3 **ABOUT YOUR PRODUCT ROBUSTNESS AGAINST ATTACKS**	What kind of functional testing are you doing ?	standardized; positive and negative test suite	Standardized test suite	Internal
	Are you familiar with Attack quotation ? (Measurement of attack difficulty)	I am aware of attack quotation tables and use them	I am aware of attack quotation tables but don't use it	I dont know
	How do you manage the security issues?	Security issues are tracked and have a dedicated policy	Security issues are collected as any other defects	Nothing is set
	Do you monitor public vulnerabities (Owasp, CVE, Conferences,...)	Yes ,included in a process	Sometimes	No
	Have you alredy performed some Robustness Testing?	Third party (black/white box)	internal	No

Witekio AN AVNET COMPANY SYNACKTIV INTERNET OF TRUST