



LCIE

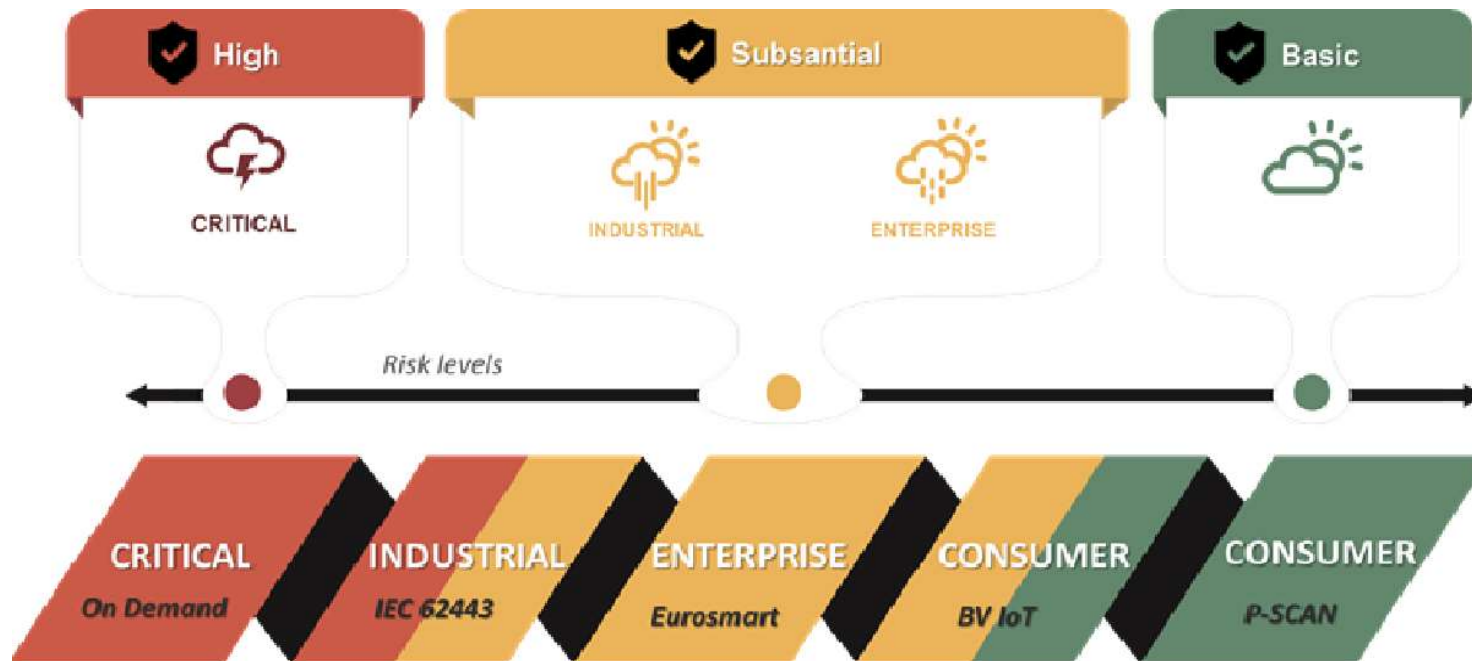
CONSUMER IOT DEVICE BV CYBERSECURITY EVALUATION SCHEME

BY LCIE BUREAU VERITAS



OVERVIEW

SECURITY CERTIFICATION DEPENDING ON SECURITY LEVELS

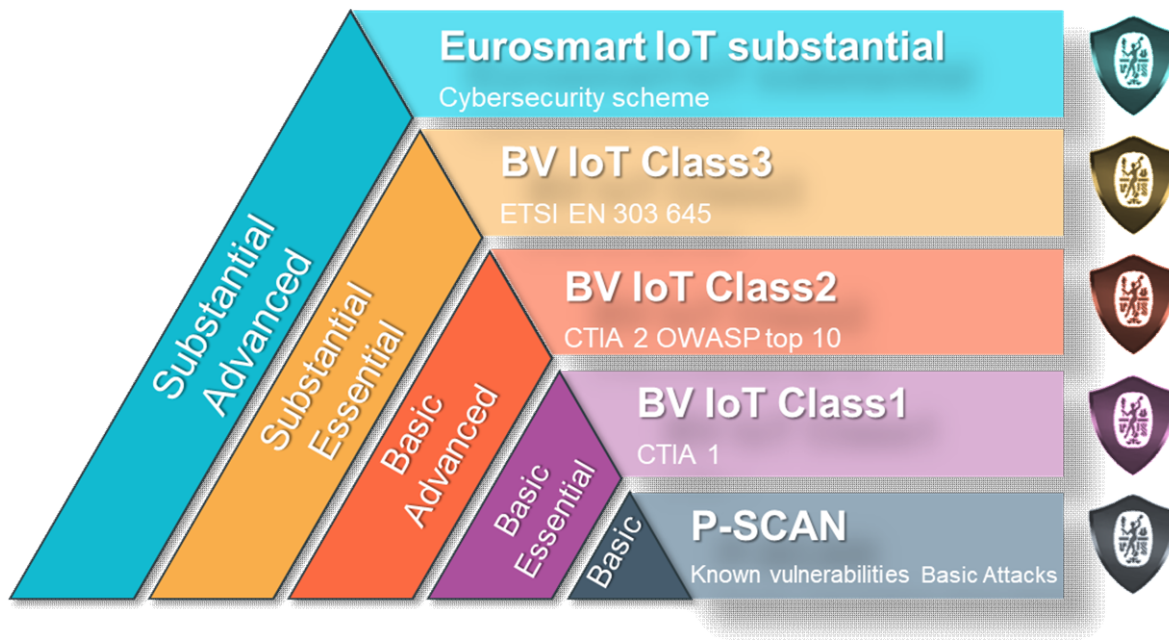


BV provides a complete set of services for the cyber certification of products.

- ✓ For products requiring **High** and **Substantial** level of security, Bureau Veritas provides certifications based on worldwide recognized certification schemes.
- ✓ For consumer product, Bureau Veritas defined its own certification scheme based on recognized standards and guidelines. ***BV IoT device cybersecurity certification scheme***



OVERVIEW CONSUMER MARKET IOT SECURITY LEVELS



Bureau Veritas defines 5 IoT security Levels

To answer the market demand to:

- ✓ Provide consumers with cybersecurity levels that can be compared
- ✓ Cover the coming regulations
- ✓ State compliance with existing guidelines

3 classes of security requirements have been defined as part of the BV IoT certification scheme

BUREAU VERITAS IOT DEVICE CYBERSECURITY EVALUATION METHODOLOGY BY CLASS

✓ CLASS 1



Basic Essential

5 days evaluation

- BLACK BOX,
- PUBLIC DOCUMENTATION,
- DECLARATIONS
- VULNERABILITY SCANNERS

✓ CLASS 2



Basic Advanced

10 days evaluation

- GREY BOX,
- INTERNAL DOCUMENTATION,
- SECURITY FUNCTIONS TESTING

✓ CLASS 3













Substantial Essential

15 days evaluation

- GREY BOX
- ADDITIONAL AND DEEPER
- SECURITY FUNCTIONS TESTING
- BASIC PENETRATION TESTING

CLASSIFICATION BY PRODUCT EXAMPLES

Products example		Market	Services	Level
<ul style="list-style-type: none"> Smart light, Connected appliances Washing machines Wearables Smart speaker Environment sensors, smart button 	 	RETAIL	BV IoT Class1	 Basic Essential
<ul style="list-style-type: none"> Connected children's toy Smart home assistants Smart Camera Connected Thermostat / Smart Air Quality Tracker Smart Navigation System Smart door bell TV Home automation Fridges 	  	CONSUMER	BV IoT Class2	 Basic Advanced
<ul style="list-style-type: none"> Connected safety-relevant products such as smoke detectors Door Locks Connected home automation and alarm systems Smart Meters / Smart Thermometer Blood pressure monitor Drones 	 	CONSUMER	BV IoT Class3	 Substantial Essential

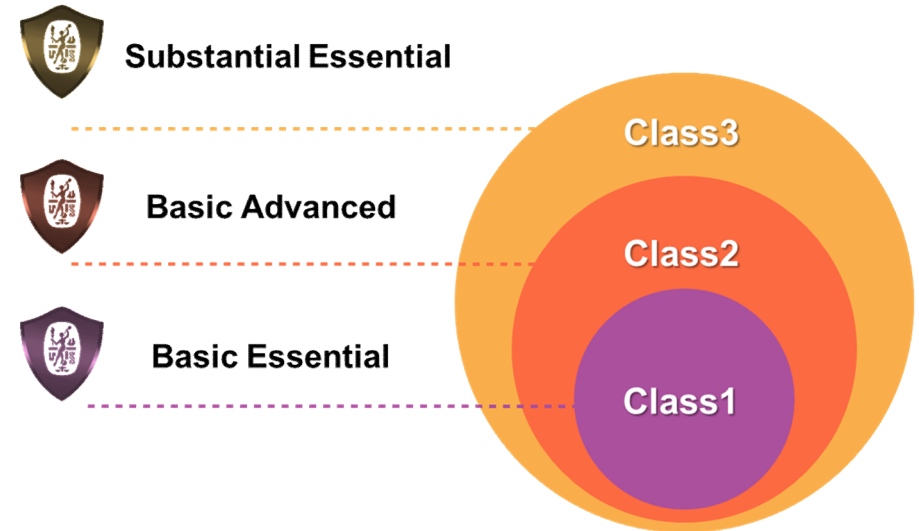
SECURITY REQUIREMENTS REFERENTIAL DOCUMENT STRUCTURE

A class is defined by a collection of security categories

- For each category, one or several requirements are defined
- Each requirement will be verified by one or several Test Cases by Bureau Veritas

Class requirements are cumulative

- A class encompasses previous one (s), increasing the assurance of previously existing one.
- Adding some new security categories which only appear from this level.
- Existing category can be completed with additional requirements to increase the insurance level.



SECURITY LEVEL **BASIC ESSENTIAL** BUREAU VERITAS IOT, **CLASS#1**

✓ **Consumer**

Main Objective:

Regulation Minimal requirements



Basic Essential

Class#1			
ID	Category	Scope	Description
1	Passwords management	Product	No universal default passwords.
2	Keep software up to date	Product	Software shall be up to date and updatable (patch or release).
3	Securely store sensitive data	Product	No storage of sensitive data in plaintext or publicly accessible.
4	Minimize exposed attack surfaces	Product	All open ports and services are documented and justified. No debug ports available.
5	The initial state is secure	Product	Default parameters provide a secure initial state.
6	Administrator and user guidance analysis	Env.	Which includes at least : Terms of Service and Privacy Policies, Hot line, a mean to report vulnerabilities, the support period and the consistency with the DUT.
7	Third-party components management	Env.	Versions of libraries, external components used.
8	Unique reference of the device	Env.	A unique reference of the certified device (HW/SW) is needed.
9	Resistance to known vulnerabilities	Product	Resistance of the software application of the device to known vulnerabilities. Use of P-SCAN

CLASS#1 defines 9 security categories

SECURITY LEVEL **BASIC ADVANCED**

BUREAU VERITAS IOT, CLASS#2

✓ **Consumer**
 Main Objective:
 Compliance to guidelines



Basic Advanced

Class#2		
ID	Category	Description
1	Passwords management	No universal default passwords
2	Keep software up to date (patch or release)	Tests in vendor's premises (vendor must provide proof elements).
3	Securely store sensitive data (passwords, ...)	No storage in plaintext or publicly accessible
4	Minimize exposed attack surfaces	(1) All open ports and services are documented and justified; (2) No debug ports available.
5	The initial state is secure	Default parameters provide a secure initial state.
6	Provide Administrator and User guidance	That includes : (1) Terms of Service and Privacy Policies; (2) Hotline; and (3) a mean to repport vulnerabilities.
7	Implementation and known vulnerabilities of third components	All third party components are documented and tested for existing vulnerabilities
8	Unique identification of the device (certified version)	Unique ID for a certified version (HW/SW).
9	Resistance to known vulnerabilities	Resistance of the software application of the device to known vulnerabilities
10	Authentication and Access Controls	Roles within device must be identified and isolated.
11	Protection of Data in Transit	Verify data are transmited signed encrypted,
12	Personal data management (RGPD)	Personnal data are identified.
13	Data input validity	Verify that target handle correctly malformed and/or unattended inputs.

CLASS#2 defines 13 security categories



SECURITY LEVEL ***SUBSTANTIAL ESSENTIAL*** BUREAU VERITAS IOT, CLASS#3

✓ **Consumer**
Main Objective:
Compliance to guidelines



Substantial Essential

Class#3		
ID	Category	Description
1	Passwords management	No universal default passwords
2	Keep software up to date (patch or release)	Tests in CAB's premises with vendor support.
3	Securely store sensitive data (passwords, ...)	No storage in plaintext or publicly accessible
4	Minimize exposed attack surfaces: no debug port available	(1) All open ports and services are documented and justified; (2) No debug ports available.
5	The initial state is secure	Default parameters provide a secure initial state.
6	Provide Administrator and User guidance	That includes : (1) Terms of Service and Privacy Policies; (2) Hotline; and (3) a mean to report vulnerabilities.
7	Implementation and known vulnerabilities of third components	All third party components are documented and tested for existing vulnerabilities
8	Unique identification of the device (certified version)	Unique ID for a certified version (HW/SW).
9	Resistance to known vulnerabilities	Resistance of the software application of the device to known vulnerabilities
10	Authentication and Access Controls	Roles within device must be identified and isolated.
11	Protection of Data in Transit	Verify data are transmitted signed encrypted
12	Personal data management (RGPD)	Personal data are identified, protected and maintained periodically.
13	Data input validity	Verify that target handle correctly malformed and/or unattended inputs.
14	Secure Boot	Verify the integrity of software executed through a secure boot process.
15	Protection of Data at Rest	Device must implement an encrypted file system (or equivalent).

CLASS#3 defines 15 security categories



WHICH CLASS TO CHOOSE

HOW TO DECIDE, EXAMPLE OF CRITERIA

The manufacturer should ideally perform a risk analysis to identify which security functions should be implemented and therefore choose the right class for the certification. Otherwise he can decide based on simpler criteria the most suitable class

Class#1 For IoT products that operate in a non-sensitive environment, in which the common usage is not security oriented.

- Limited impact if the object is hacked
- Connected to a local network only
- Limited or no private data

Class#2 For objects that need a first level of security, which operate in a sensitive environment.

- Serious and visible impact in case of service disruption or significant financial impact.
- Unauthorized disclosure of information shall be expected to have a serious adverse (private or sensitive data)
- Indirect connection to the web (i.e. connected to the wifi home box)

Class#3 Reserved for products that need a real security assurance (substantial security level)

- Safety, security or serious financial impact if the object is hacked
- Direct connection to the web
- Unauthorized disclosure of information shall be expected to have a critical adverse (very sensitive data)
- Disruption of access to this device shall be expected to have a critical adverse effect on the service or the user.



BUREAU VERITAS IOT CYBERSECURITY CERTIFICATION PROCESS

- ❑ *The manufacturer chooses a class of requirements and submit the device to be assessed.*
- ❑ *The manufacturer submit and Application Form to ask for the certification, which becomes the contract for the service.*
- ❑ *Additional information (questionnaire, evidences) are requested to the device vendors as per described in the BV cybersecurity IoT certification scheme and the Bureau Veritas IoT device cybersecurity Evaluation Methodology*
- ❑ *The Assessor verify the conformance of the devices to the selected requirements via testing, auditing or inspection*
- ❑ *In case of successful evaluation the certificate is deliver to the manufacturer*
- ❑ *Surveillance is performed for the Basic Advanced and Substantial Essential certificates*

BUREAU VERITAS IOT CYBERSECURITY

INPUTS NEEDED FROM THE MANUFACTURER

Depending on the Class chosen the device manufacturers have to provide numbers of inputs. This inputs are defined in a specific document that is provided to the manufacturer priori to the evaluation.

- DUT samples : 5
- Documents evidences : test reports, design documents ..
- Answer to technical questionnaires
- Access to the developer for questions
- Access to the test Lab

BENEFITS



Consumer reassurance and brand advantage:

Consumers are increasingly concerned about product security. Bureau Veritas robust testing and certification program give consumers confidence that a client's product is secure, giving a significant sales advantage to certified products.

[Visit our Cybersecurity database](#)



Helping meet regulatory requirements:

Even basic regulatory requirements imply a direct liability from manufacturers. Bureau Veritas IoT solutions Level 1 & Level 2 give you the way to comply with them and mitigate your risks.



Verify State of the Art security:

Bureau Veritas IoT solutions Level 2 to Level 5 allow you to verify that the security implemented in the product is adequate for its usage and provide the right level of confidence.



Worldwide certification:

Bureau Veritas has a presence in every major country around the world with 1,400 offices and laboratories and as a trusted partner. Bureau Veritas provides a global footprint and certificate recognition.





L C I E

THANK YOU

