EUROSMART

The Voice of the Digital Security Industry

[INFORMATIVE ANNEXES]

ANNEX I – e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE

EXECUTIVE SUMMARY

The EU's new Cybersecurity Act aims to improve EU cyber resilience and response by building upon existing instruments that keep networks and information systems secure. With the Commission's proposal, the current system is reformed to make ENISA the centre of the operation of setting up an EU cybersecurity certification framework.

European Cybersecurity Certification Framework could help creating a single cybersecurity market for the EU. A harmonized approach at EU level defines mechanisms that establish EU-wide cybersecurity certification schemes which assess the ICT (Internet and Communications Technology) processes, products and services and make sure they comply with specified security requirements.

Each certification scheme should include items such as subject-matter and scope, type of categories of ICT processes and products and services that it covers. It should also detail how the certification scheme in question suits the needs of the target groups. Where that's applicable, plans should also include assurance levels and any specific or additional requirements that would guarantee that conformity assessment bodies who are evaluating the cybersecurity requirements are technically competent to do so.

This pre-study assesses the feasibility of a candidate certification scheme for the Internet of Things (IoT) devices with a focus on the Substantial security assurance level as defined by the Cybersecurity Act. At this level of assurance, the certification is intended to minimize the risks of successful attacks commonly taking advantage of poor design in IoT devices bringing severe consequences to consumers and vendors, due to ineffective security controls. It is indeed vital that IoT devices have security designed-in and verified-in from the outset.

Since these IoT Devices at the low end of the range may have security features constrained by cost, available processing power and performance, size, type of power source, the candidate Certification Scheme considers the trade-off between such constraints, the risks and the cost of certification.

Finally, the proposal is foreseen to become more generally an alternative to current product certification schemes like the Common Criteria which are static regardless the Target of Evaluation specificities and operational environment. Toward a more adaptive approach allowing to configure some of the scheme key elements to adapt them to the use case while remaining consistent.

Author: Roland Atoui – Red Alert Labs

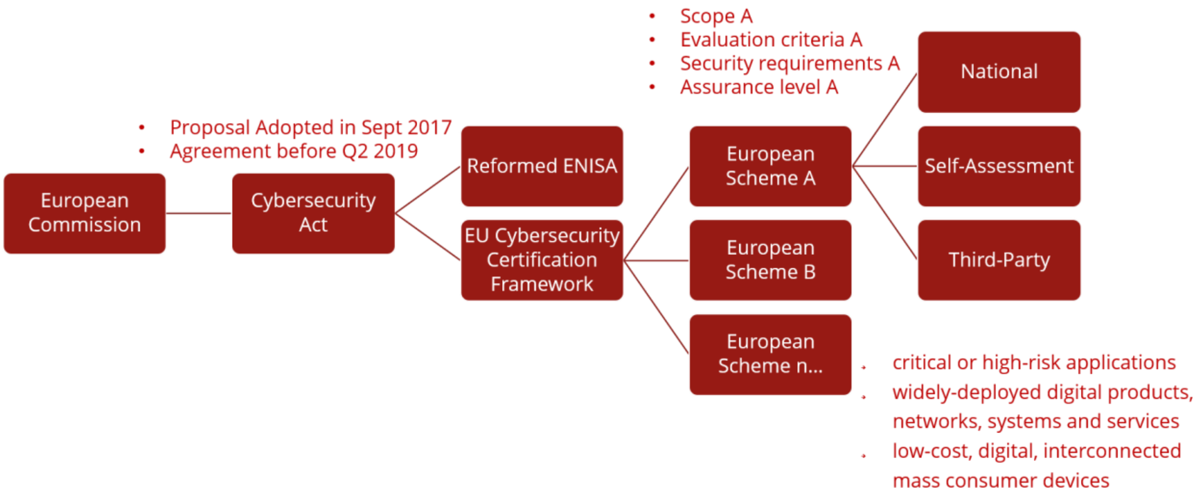
Contributors: François Guerin – Gemalto, Eric Vetillard – NXP, Sylvie Wuidart – STM, Martin Schaffer – SGS, Gisela Meister - G&D, Stefane Mouille - Eurosmart

Date	Version	Description of changes
15/08/18	V0.1	Initial version created
20/08/18	V0.2	Chapter 1 and 2 completed
27/08/18	V0.3	Chapter 3 structuring
29/08/18	V0.4	Completed Chapter 3 Including François Guerin – GEMALTO comments
31/08/18	V0.5	General updates and started Chapter 4
13/09/18	V0.6	Updates and integration of comments (STM + NXP) following ENISA meeting on the 6th of September
21/09/18	V0.7	Completed Chapter 4 – TODOs: Executive Summary + Pilot Project and Timeline Updates.
25/09/18	V0.8	Added general comments collected during the last conf-call with the members.
01/10/18	V1.0	Final version released + slight updates to the executive summary (03/10/18)

Contents

1 Introduction

The European Commission proposed an EU Regulation called the "European Cybersecurity Act" mandating the Agency for Network and Information Security (ENISA) to create a framework for establishing European Cybersecurity Certification Schemes for ICT products and services. The goal is to ensure an adequate level of cybersecurity of ICT products and services within the EU member states.



Security Certification of ICT products in Europe has been led by the evolution of the Common Criteria (ISO/IEC 15408), the work of SOG-IS and different private initiatives.

While these schemes proved to be successful in some market sectors, there seems to be no coherent and holistic approach addressing the Internet of Things horizontal market and specifically IoT devices.

This document is a pre-study of a new Certification Scheme Candidate addressing IoT Devices and providing a Substantial level of security assurance as defined in the Cybersecurity Act.

Its goal is to draw only the principles of the Certification Scheme Candidate and get a clear plan on its implementation. This document will be presented to ENISA to set a common expectation.

EUROSMART will work in close collaboration with ENISA and main stakeholders to have this candidate scheme ready by July 2019.

1.1 Certified Conformity Assessment

ICT product vendors are used to make claims about the security of their products or solutions. Without some proof, customers would have to take the vendor's word that their claims are true. Certified Conformity Assessment provides value to customers by having independent third-party evaluates the vendor claims against specified security requirements. This is the basis for trusting the results of the assessment.

After a successful evaluation, a certificate is issued by a Conformity Assessment Body which could be a private or a public body.

Customers can gain even more confidence in evaluation results if evaluation is performed by independent third-party with a proven credibility. This means that this third-party has also undergone some assessment by a National Accreditation Body (NAB).

When the CAB is represented by a government, this qualifies as a National-assessment.

1.2 EU Cybersecurity Certification framework

The EU Cybersecurity Certification framework will be composed of several certification schemes addressing different types of ICT products, systems, processes or services and will be consider the following principles among others:

- Conformity Assessment with standard security requirements that will be defined by scope
- Three levels of security assurance (basic, substantial and high)
- Specific evaluation methodologies and criteria
- The certification is voluntary, unless otherwise specified in EU law.
- May define Terms of use of Marks/Labels
- Defines requirements for maintenance and extension validity period of certificates

1.3 Proposed Certification Scheme

The proposed Certification Scheme refines the EU Cybersecurity Certification Framework following the principles listed above and based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service e.g. Secure Elements or IoT Devices.

The certificate will attest that an IoT device, for instance, have been certified in accordance with such a scheme comply with specified cybersecurity requirements. The resulting certificate will be recognised in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service

A Certification Scheme is a systematic organisation covering Evaluation and Certification of ICT products under the authority of ENISA to ensure that high standards of competence and impartiality are maintained, and that consistency is achieved during the whole certification process.

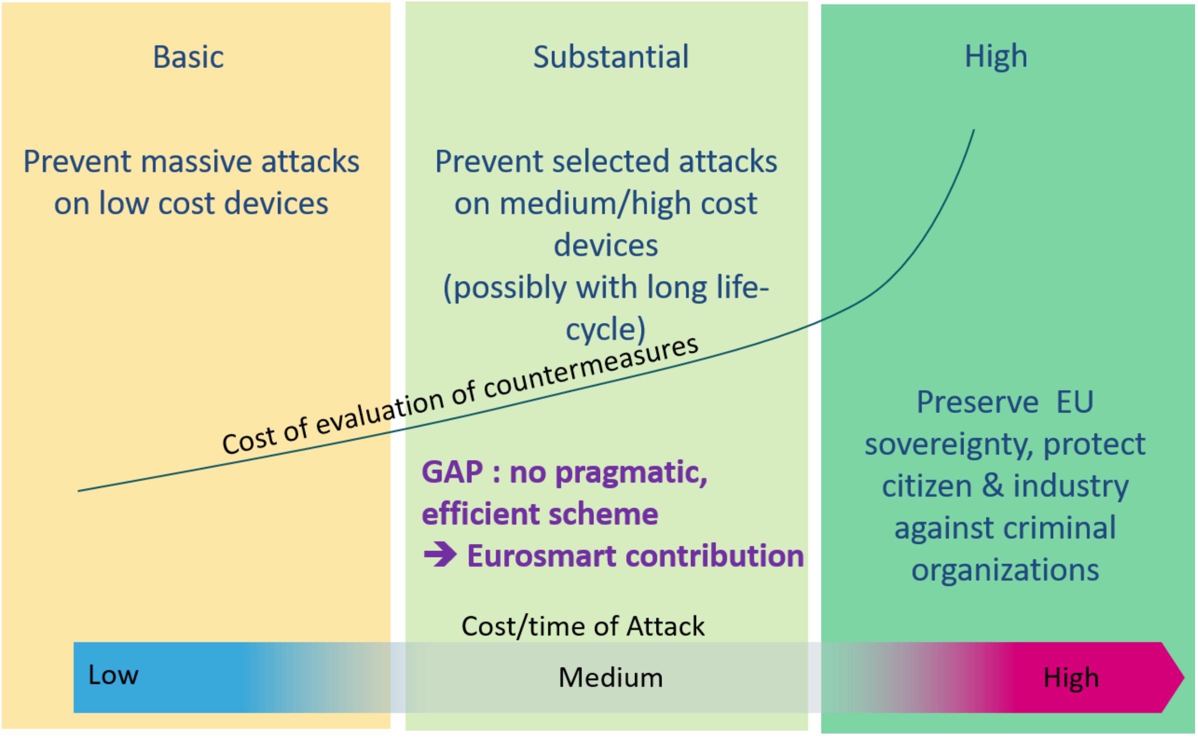

Basic
Substantial
High
Prevent massive attacks on low cost devices
Prevent selected attacks on medium/high cost devices (possibly with long life-cycle)
Cost of evaluation of countermeasures
GAP : no pragmatic, efficient scheme
➔ Eurosmart contribution
Preserve EU sovereignty, protect citizen & industry against criminal organizations
Cost/time of Attack
Low
Medium
High

Figure 1: Security Evaluation from Basic to High

1.4 Roles & Responsibilities

• A Conformity Assessment Body (CAB)

A Conformity Assessment Body (CAB) that has been accredited by a National Accreditation Body (NAB) is an organisation, which carries out Evaluations, independently from the developers of the ICT products. A CAB is responsible for carrying out Certification and overseeing the day-to-day operation of an Evaluation.

• National Certification Supervisory Authority (NCSA)

National Certification Supervisory Authority (NCSA) is a representative of a national cybersecurity certification authority. Their main task is to implement and supervise some specific certification schemes covering ICT processes, products and services. Typically, schemes requiring a High level of security assurance. NCSA should handle complaints lodged by natural or legal persons in relation to certificates issued by conformity assessment bodies established in their territories. Moreover, they should cooperate with other certification supervisory authorities or other public authorities by sharing information on possible non-compliance of ICT products and services with the requirements of this Regulation or specific cybersecurity schemes.

• National Accreditation Body (NAB)

A National Accreditation Body (NAB) is responsible of CABs' accreditation. NABs are responsible of assessment and continued monitoring of the competence of CABs. NABs shall possess the relevant knowledge, competence and means to properly perform audits to determine if a CAB has the technological knowledge, experience and the ability to carry out assessment.

• Certification Scheme Manager (CSM)

A Certification Scheme Manager is carried out by the technical group that created and proposed the Certification Scheme to ENISA. Its main responsibility is to create, maintain and update the Certification Scheme accordingly. It shall operate within an industrial consortium composed of relevant Certification Scheme Users.

• Certification Scheme User (CSU)

Certification Scheme User is a Vendor adopting the Certification Scheme or a sponsor financing the Certification Scheme process.

1.5 Certification Scheme Users (of the proposed scheme)

This proposed Certification Scheme is addressed to Vendors of IoT Devices (as defined in Section 2.3). These vendors could be the integrators[1] of different components purchased through components[2] vendors[3].

[1] Integrators such as APPLE, AMAZON, FOX-TECH, LEGRAND, PHILIPS, SENS'IT, NEST, LIBELIUM, etc.

[2] Components could be for instance the Transceivers, SoCs, Modules or Secure Elements, etc.

[3] Components Vendors such as STM, NXP, GEMALTO, TEXAS INSTRUMENTS, SILICON LABS, MICROSHIP, TELIT, etc.

1.6 Purpose & Principles

The purpose of the proposed new certification scheme is to ensure that IoT devices certified under such a scheme comply with specified requirements supported by the industry with the aim to protect the availability, authenticity, integrity and confidentiality of stored or transmitted or processed data or the related functions of or services offered by, or accessible via IoT devices throughout their life cycle.

The targeted level of assurance within the meaning of the Cybersecurity Act regulation is **substantial**.

Note that IoT devices could be certified for a High level of security assurance but this remains out of the scope of this candidate certification scheme.

1.7 Certification Process

The Certification process follows typically the following steps:

1. The Developer develops an IoT Device.
2. The Sponsor (who can be developer itself) requires a certificate for the developed IoT Device for instance, and hence turns to a Conformity Assessment Body (CAB) accredited by a National Accreditation Body (NAB).
3. The CAB carries out the Evaluation by assessing the Target of Evaluation (ToE) against predefined security requirements.
4. The CAB finally summarises the result of the Evaluation and confirms the overall results by issuing the Certificate.

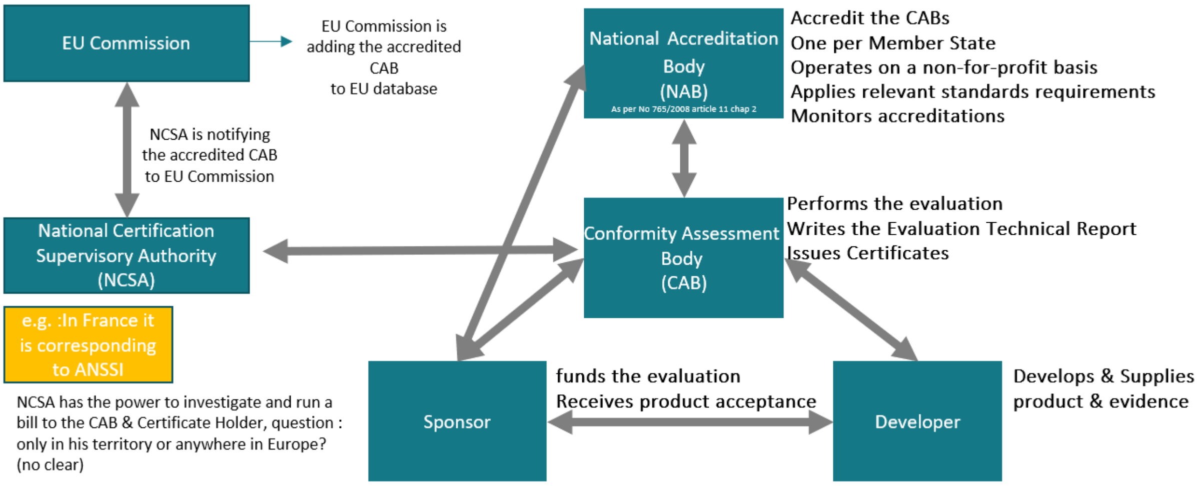

EU Commission
EU Commission is adding the accredited CAB to EU database
National Accreditation Body (NAB)
As per No 765/2008 article 11 chap 2
Accredit the CABs
One per Member State
Operates on a non-for-profit basis
Applies relevant standards requirements
Monitors accreditations
NCSA is notifying the accredited CAB to EU Commission
National Certification Supervisory Authority (NCSA)
Conformity Assessment Body (CAB)
Performs the evaluation
Writes the Evaluation Technical Report
Issues Certificates
e.g. :In France it is corresponding to ANSSI
NCSA has the power to investigate and run a bill to the CAB & Certificate Holder, question : only in his territory or anywhere in Europe? (no clear)
Sponsor
funds the evaluation
Receives product acceptance
Developer
Develops & Supplies product & evidence

Figure 2: Participants of an Evaluation and Certification Process

1.8 Benefits of a European Certification Scheme

We see at least two major benefits for having a European Certification Scheme

1. **Access to the digital single market at a lower cost:** Mutual recognition of certificates by the member states helps avoiding market defragmentation and allow vendors to get access to the digital single market. In addition, a well-established certification scheme will reduce the time and cost for vendors and simplifies the procedures.

2. **Increase Trust:** This is not just about end-user's trust but also mutual trust between all stakeholders (component suppliers, integrators, operators, etc.) which is a condition to ensure the development of a business and sustainable economy.

1.9 Key Concepts & Definitions

Using a common language is very important to formalize the concepts and leverage more objective results. This scheme will be based on existing definitions as defined by the Common Criteria and ECSO Meta-Scheme Approach[4].

• Target of Evaluation (ToE)

This is comprised of the software and hardware under evaluation. This scheme will address IoT device as a ToE based on a predefined reference architecture.

• General Protection Profile (GPP)

This specification will be based on a generic security risk analysis approach of an IoT Device reference architecture without considering a specific type of data or a context for risk calculation. The main output of this document will be a list of security goals/objectives qualifying the need to counter threats identified on a typical IoT device.

• Security Profile/Protection Profile (SP)

This is a refinement of the GPP to address specific problem definition of a type of ToE (thermostat, smart cam, etc.) while considering the type and sensitivity of data and the context of the operational environment (e.g. Consumer, Enterprise, Industrial) and the risk factor.

Their definition is a step towards an economic way of dealing with security evaluation. They help to scale security controls and security-related process activities in accordance to the identified risks, i.e. to spend most effort where the highest risks are.

Security Profiles may be agreed on and standardized for certain product classes.

A standardized security profile saves a detailed risk analysis for every new product instance. It provides an accepted standard on security properties of a product.

• Security Targets

This is where security functionality specific for a given product are identified and mapped to the security goals.

• Security Goals/Objectives

The Security Goals are statements of an intent to counter identified threats and/or satisfy identified security policies on the environments and/or assumptions

• Security Requirements

These are the security measures to be implemented by a security functionality and contributes in achieving security goals. This step is optional, but it becomes valuable when it translates the security goals into a standardised language.

[4] European Cyber Security Certification A Meta-Scheme Approach – December 2017

- ### Security Assurance & Level

This is the description of how assurance is to be gained that the ToE meets the security goals/requirements.

As defined in the Cybersecurity Act, assurance levels provide a corresponding degree of efforts for the evaluation of a TOE and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to mitigate or prevent cybersecurity incidents. Each assurance level should be consistent among the different sectorial domain where certification is applied.

- ### Substantial Assurance

Assurance level “substantial” provides assurance that the ToE meet the respective security requirements including security functionalities and they have been evaluated to a level which aims to minimise known cyber risks, cyber incidents and cyber-attacks carried out by actors with limited skills and resources. The evaluation activities shall include at least: reviewing the non-applicability of publicly known vulnerabilities and testing that the ICT processes, products or services correctly implement the necessary security functionality; or where not applicable they shall include substitute activities with equivalent effect

2 IoT & Target of Evaluation

2.1 IoT Definition

For ENISA, IoT is an emerging concept comprising a wide ecosystem of interconnected services and devices, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components. The “Things” collect, exchange and process data to dynamically adapt to a specific context, transforming the business world and the way we live. IoT is tightly bound to cyber-physical system and, in this respect, safety implications are pertinent.

2.2 IoT Infrastructure Reference Architecture

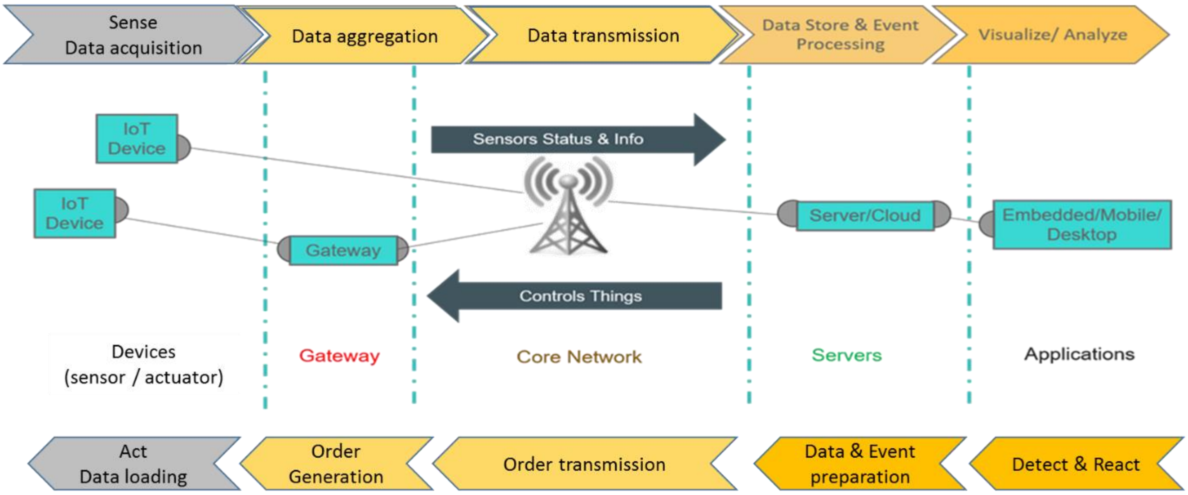


Figure 3: IoT Infrastructure Reference Architecture

2.3 IoT Device Definition

An IoT Device is a "Thing" as per the IoT definition above that is mainly composed of:

- a Hardware including microcontrollers, microprocessors, mother board, ICs, physical ports.
- A Software including an embedded OS, its firmware, programs and applications
- Sensors which detect and/or measure events in its operational environment and send the information to other components
- Actuators which are output units that execute decisions based on previously processed information

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, with the ability to monitor and transfer data over a network without requiring human-to-human or human-to-computer interaction.

2.4 IoT Device Typical Components

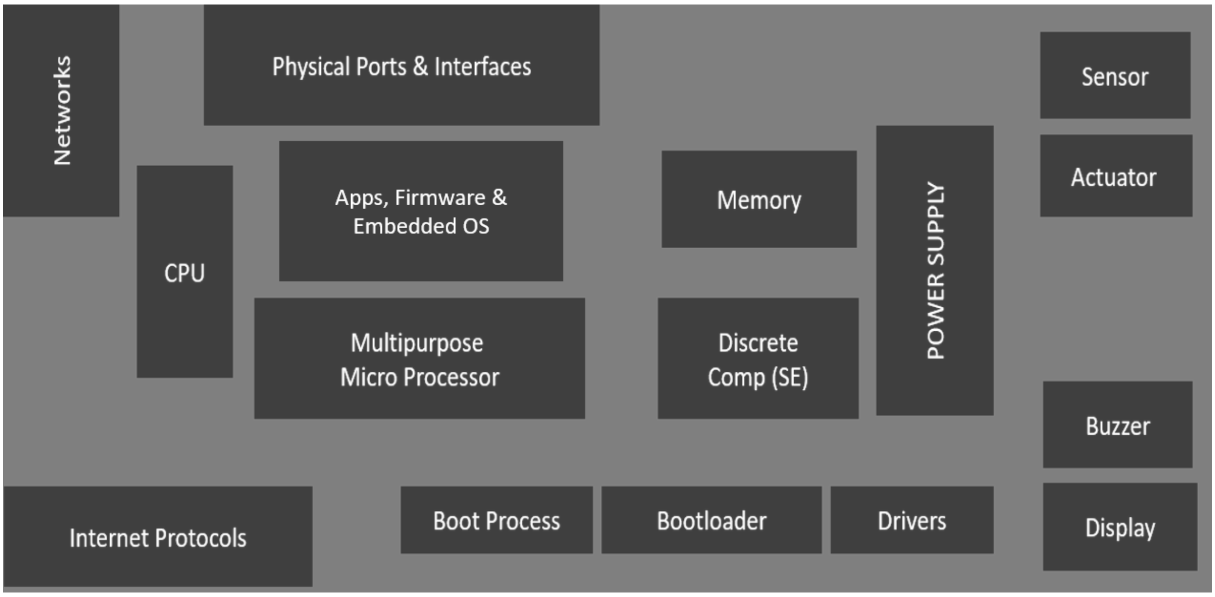


Figure 4: IoT Device Reference Architecture

IoT Devices could have the following characteristics:

- Embedded Devices
- Linux Based Devices
- Resource Constraint Devices
- Microcontroller based devices with flash/firmware
- Microprocessor based devices
- Devices with Medium Memory Capacity (1MB and above)
- Can be used with or without a TPM or a Secure Element (SE)

• Data Flow

Data is pervasive throughout the IoT system. Each set of data has a different lifecycle, time of relevancy and potential risk associated with its compromise. The threat may result from its modification, interception or duplication. The effects of attacks on data vary from immediate change in system behaviour to subtler negative behaviour in the future.

The data protection strategies for each type of data fall into three categories:

- **Data-at-Rest (DAR)** is data in persistent storage, for example, in a solid-state disk (SSD) on an edge device.
- **Data-in-Use (DIU)** is data placed in non-persistent storage such as random-access memory (RAM) and CPU caches and registers.
- **Data-in-Motion (DIM)** is data moving between two or multiple IoT devices

2.5 Operational Environment

In this part, it is necessary to specify the Operational Environment where the IoT device is intended to work. Indeed, the knowledge of the application area of the product is essential to set its security objectives and subsequently the corresponding security functions.

Example: Ensuring secure communication in connected equipment that handles financial transactions is obviously not achieved in the same way as for a smart calendar that connects to the user's smartphone to remind them of their appointments. Same goes for a connected camera that could be installed at home (indoor environment) and the one that is installed on the side of the road (outdoor environment) the security requirements would vary depending on the operational environment.

Therefore, we invasion 4 generic types of Operational Environments:

- Consumer (Basic to Substantial)
- Enterprise (Substantial)
- Industrial (Substantial to High)
- Critical (High)

Operational Environment	Types of IoT DEVICES
• **Consumer & Home**	Connected Light bulbs, Connected TVs, eReaders, Power Systems, Dishwashers, lighting, Washers/Dryers, Alarm systems, Humidity sensors, etc.
• **Enterprise**	Storage, Routers, Thermostat, Switches, PBXs, CCTV, Alarm systems, etc.
• **Industrial**	Connected Pumps, Valves, Vats, Conveyors, Pipelines, Motors Drives, Converting, Fabrication, Vessels/Tanks, etc.
• **Critical**	MRI, PDAs, Implants, Pumps, Monitors Telemedicine, Connected Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, road traffic sensors,

We might obtain for instance the following security goals differences to be enforced in each operational environment:

CONSUMER	• Protection against remote scalable attacks through external interfaces, Data Confidentiality, IP Protection, …
ENTREPRISE	• Secure Firmware updates/Reprogramming and Remote Access Authentication, …
INDUSTRIAL	• Local Internal Interface Access Enforced Authentication, Assets Availability, Communication Integrity, …
CRITICAL	• Firmware Integrity, Secure Booting and Physical Access Authentication, …

2.6 Assets

Here we mainly address the primary assets which are the Data.

Data can be of different types and for different purposes. Here it is classified into three types depending on its functions.

Device Data: This includes all the data that is generated by the different devices and sent to the server along with the control signals that is sent back to the devices from the cloud server.

Security Data: This includes all the data that is generated and used for implementing different security mechanisms in the system

Configuration and Monitoring Data: This includes all the data that is required for the configuration, management and monitoring of the different components of the system.

The secondary assets could be representing the physical components of the IoT device or those part of its operational environment.

2.7 Threats

After all the assets and attack points are identified, all the potential threats are listed along with its impact and type.

2.8 Vulnerabilities

After all the potential threats are identified, the vulnerabilities that can lead to the threats are identified.

2.9 Substantial Risk Rating

Depending on the threat agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the IoT device business application, security risk rating are qualified. We could one of the existing methodologies such as OWASP Risk Rating, DREAD, EBIOS, ISO27005, etc.

2.10 Security Goals

This is a snapshot of some security goals that could be considered as the basis of the GPP

- Data Integrity (DAR) (DIU) (DIM)[5]
- Data Confidentiality (DAR) (DIU) (DIM)
- Identification & Authentication
- Access Control
- Data Availability
- Cryptography
- Physical Security
- Secure Storage
- Secure Communication
- System Hardening
- Security Audit
- Secure Data Management

[5] Note that DAR and DIM integrity and confidentiality could be covered by the secure storage and secure communication goals.

- Non-repudiation
- Privacy

Based on risk-based methodology we will be able to classify the security goals into 3 levels:

Security Goal (Sample)	Basic	Substantial	High
Strong Authentication		X	X
Firmware Integrity			X
Communication Integrity			X
Strong Encryption		X	X
Data Confidentiality		X	X
IP Protection	X	X	X
Data Availability		X	X
Data Privacy	X	X	X
Human Safety			X

2.11 Security Functions

These are few examples of security functions or measures that could be part of the ToE satisfying security goals.

- Data Encryption
- Secure Firmware Updates
- Secure roll-back
- Secure Keys generation
- Intrusion Detection
- Secure logs
- Unique ID

Security Functions/Requirements (sample)	BASIC	SUBSTANTIAL	HIGH
Secure Manufacturer-based Identity & Certificate Storage		X	X
Secure Storage (Tamper Resistant)			X
RNG (FIPS or AIS)		X	X
SHA-256 at least		X	X

Secure Onboarding		X	X
Secure Firmware/SW update (digital signature)		X	X
Secure Event Logging		X	X
Limited Data Collection	X	X	X
End User Data Removal	X	X	X
Secure Cloud-Based Management Services		X	X
Active Product Incident Response Team		X	X
Secure Development Lifecycle (SDLC)			X
Data Privacy (Manufacturing)	X	X	X

3 CERTIFICATION STANDARDS – GAP ANALYSIS

3.1 Background

With a 19 trillion-dollar market size by the year 2020, it's no surprise why the Internet of Things (IoT) manufacturers are racing against time to create IoT products for consumers, enterprises, and governments. The merging of cloud, big data, wireless technology, endpoints, and the Internet of Things, can create a critical situation for security experts. More than 50 billion IoT devices will be made available across all industries including automotive, education, home appliances, consumer electronics, banking, medical, manufacturing, and more.

However, the development and implementation of IoT-based devices is anything but a risk-free zone. Plenty of risks abound, especially in terms of security.

Plenty of schemes are on the table being hotly discussed, but as it stands, there has been no proposal that has convinced the industry to get adopted and therefore the same Schemes such as Common Criteria, CSPN and CPA are being used.

Given the swift product life-cycle and flexible nature of business operations, many IoT experts are calling for improvements to the existing security certification schemes.

3.2 How to compare security certification schemes?

You should note that Security is multidimensional, so we can measure it using a simple ruler.

But like all standard measurement methods, methodologies and metrics have been invented to measure security.

So far, several methodologies have been used to qualify the level of resistance to attacks on IT products including hardware and software in the perimeter. For example, Common Criteria (ISO 15408), CSPN, FIPS 140-2, FIDO, etc.

These methodologies could be differentiated by the following characteristics:

- **Recognition**: global, national, European or an industrial community
- **The formalism:** from the definition of the security requirements to the execution of the tests, the methods could have a precise formalism based on a semi-formal or formal language
- **The scope of coverage**: covering a single type of product or a multitude of products, or sometimes even a specific part of a product (e.g. cryptographic module)
- **The objectivity of the results**: allowing to repeat the same tests to have the same results, to prove the coverage of the requirements or to compare two identical products.
- **The variety of levels:** from the basic level to the high level, some methods provide a more flexible degree of granularity than others.
- **And costs:** the more effort a methodology requires, the more time the assessment will take and so the cost will be higher.

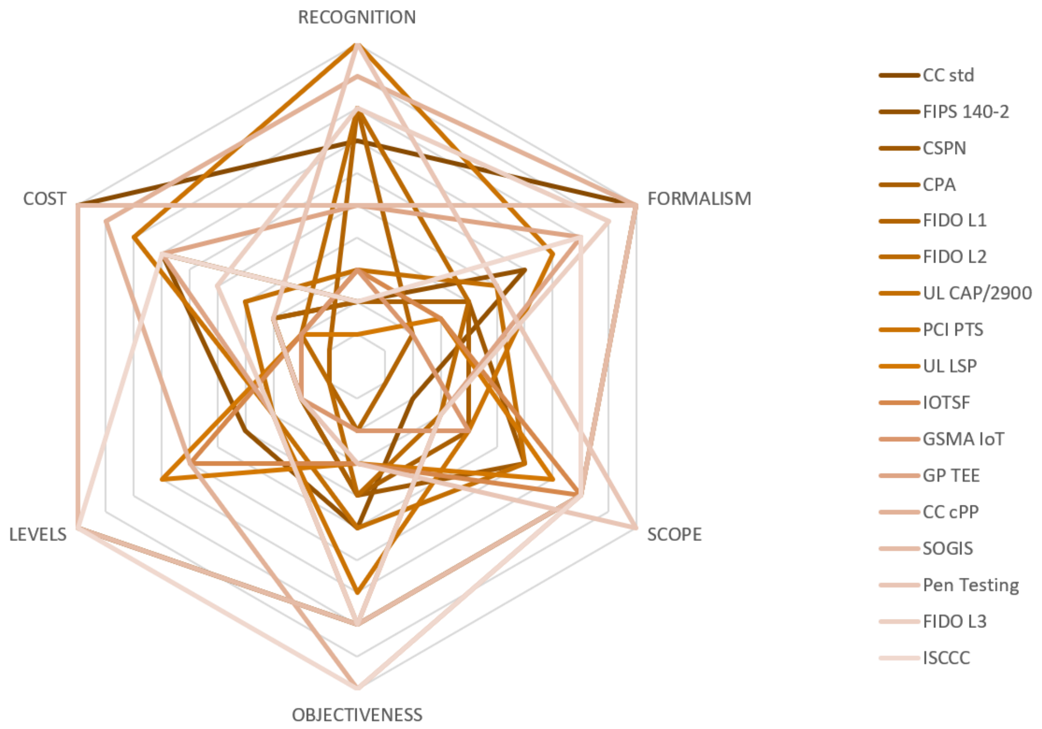


Figure 5: Certification Schemes Comparison[6]

Here are some of the gaps within the currently existing framework:

- ## COST

IT products certifications cost a considerable amount of money, take a lot of time and are often VALID for a limited time. Costs vary considerably, depending on the complexity of the product, the level of insurance coverage, etc. This includes also the preparation costs before the start of the evaluation process.

Costs for common criteria for instance are generally divided into eight areas: product design, consulting, product modification and implementation / design costs, test development, documentation, production, laboratory verification, and fees of the certification scheme. To get an idea, a CC EAL2-3 assessment will cost between 80K€ and 120K€ and could last from six months up to a year. Costs of a CSPN evaluation varies between 25K€ and 70K€ (considering that products might fail the first certification and therefore pass it twice to get certified)

Obtaining management approval to unlock a large investment required for CC assessments is essential to being able to start the evaluation project. Thus, developing a compelling business case becomes a big challenge.

This argument becomes even more complicated as developers or vendors are used to differentiating products based on their features or functionality and their costs. What drives this further is that customers or end users are not used to differentiating products based on security. And so, the manufacturing lifecycle time is minimized so it does not take time to design, test, and update security.

And when we apply it to the IoT market, the cost criteria, duration and validity become not suitable for the market of 50 billion IoT devices. There will simply not be enough resources to do it.

[6] This is based on an internal study done by Red Alert Labs reflecting more than 10 years of experience in the Certification field.

- ### RECOGNITION

Perhaps the most common refrain in IoT security certification debates is the need for a global Conformity Assessment Body thus ensuring the following benefits:

- All the different certification bodies that exist today would finally operate on an “equivalent, comparable, and competitive basis”
- End-users have the assurance that the certification is valid, no matter the size or scope of the body issuing the certificate
- It would bring the costs down for the business looking to gain security certification. As it stands, applying for numerous foreign certifications is an expensive and time-consuming process. As a result, many businesses do not pursue business in international markets

Thankfully, the European Cybersecurity Certification Framework is a great initiative addressing this gap within the EU context.

- ### FORMALISM, LEVELS, OBJECTIVENESS

The Common Criteria standardization model has been the benchmark for security certification across business sectors for over 20 years. In this time the product life cycle has shortened; businesses have become far more agile – and yet the verification process remains generic.

The CC model begins with an individual risk assessment, which sets a Security Target for the product. Each security target is usually based on a specific protection profile (PP) addressing sometimes only a part of the product. This sets the Security Functional Requirements and the Security Assurance Requirements that will be assessed by a Third-Party Evaluator following the CC evaluation methodology.

The rise of IoT companies has highlighted just how slow and vague the framework is. But what can be done about it?

What if we restructure the framework to:

- Allow rapid & agile product manufacturing life-cycle while taking care of security
- Reduce the evaluation costs and time
- Create incentive for the vendor
- Provide simple methods/metrics to the vendors
- Provide simple methods/metrics to the evaluators
- Recognize other existing evaluations methodologies and security standards
- Recognize self-assessment (for a basic security assurance level)
- Consider the full Operational Environment/Processes/Context/Domain in a System and Product approach
- Accelerate or Automate Certificates Maintenance when it is possible
- Allow the customer and the vendor to compare different products OBJECTIVELY

3.3 What about Trust Labels?

There, then to give the clear message that, the higher up we look at the stack the more products exist with developers have less clue about what they are doing. And that it is unrealistic to ask for super deep assessment for thousands of products which have a life time of approx. 1 year. Thus, a scheme needs to give credits for those who used certified bricks underneath => there needs to be an incentive: if you use certified bricks to build the IoT device, the evaluation for you will get much easier and cheaper (can be a self-assessment even), but if you don't use any certified bricks it will get longer and more expensive.

3.4 What about Trust Labels?

The use of trust labels on products could be misleading if not carefully defined. Using a general stamp to express the security risk for an assortment of complex products for instance should be defined carefully considering the different features/components that could vary from a product to another.

Therefore, defining IoT Security Profiles must be based on a smart security analysis considering the full threat modelling on the system, process and product.

Finally, the certificate statements expressed by the trusted label must deliver a clear message to the final consumer and participate to creating awareness.

3.5 Penetration Testing vs Vulnerability Scanning vs Vulnerability Assessment

These three concepts are often confused for the same service which is wrong.

Indeed, Vulnerability Scanning is an automated and high-level testing that identifies potential vulnerabilities whereas a Penetration Testing is an exhaustive, live examination intended to exploit flaws or weaknesses in the ToE. Finally, the purpose of the Vulnerability Assessment is to determine the existence and exploitability of flaws or weaknesses in the ToE including a qualification of identified vulnerabilities on the ToE.

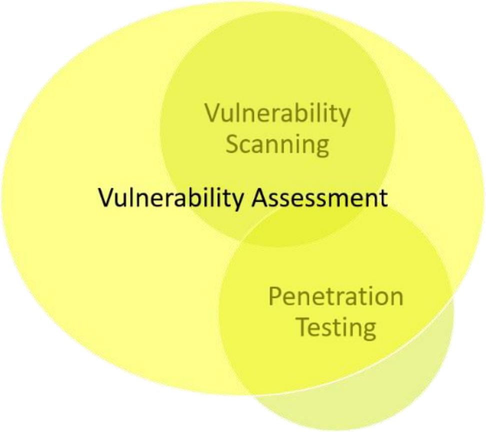


Figure 6: Vulnerability Scanning vs. Penetration Testing vs. Vulnerability Assessment

TYPE	**EXECUTION**	**ACCURACY**	**STANDARDS ADOPTION**	**TIME REQUIRED**	**RESULTS EFFICIENCY**	**COST**
Vulnerability Scanning	Automated (in general)	High look at what could possibly be exploited – public vulnerabilities	Required by Schemes such as PCI DSS, FFIEC, GLBA, etc.	Takes several minutes to several hours to be completed	Reports identifies weaknesses but may include false positives	100€ to 1K€

Penetration Testing	Live, Manual tests	More accurate and thorough results – public vulnerabilities	Required by Schemes such as CSPN, CC, Private Schemes, etc.	Takes 1 day to 3 Weeks	Rules out false positives	5K€ to 30K€
Vulnerability Assessment	Live, Manuel tests	Adds accuracy and relevancy by qualifying the vulnerabilities according to attackers profiles, means used, … sometimes considering the Identification and Exploitation phase of a vulnerability. Public and New vulnerabilities	Required by Common Criteria AVA_VAN assurance requirement, CSPN, etc.	Takes 3 weeks to 2 months	Extensive report allowing the vendor to patch the product	20K€ to 90K€

Figure 7: Finding Vulnerabilities - Criteria of comparison[7]

• Which is better for IoT Devices?

All the three tests types are great and could help in building security by design. Nevertheless, each of those tests could provide adequate assurance in meeting the security goals for IoT devices. Therefore, it all depends on the market vertical and the operational environment of IoT devices. We can estimate that for a SUBSTANTIAL security assurance level as defined by the Cybersecurity Act, vulnerability scanning and/or penetration testing carried out by actors with limited skills and resources are required at least to provide the adequate protection against known cyber risks, cyber incidents and cyber-attacks. How we calibrate between both depends on the IoT device operational environment.

3.6 Conclusion

For businesses to provide secure IoT Devices for end-users, there needs to be an adapted IoT Security Certification Scheme in place allowing a more agile evaluation process. IoT threats are only going to become more acute, and without a collective approach that promotes transparency and accuracy, there is little hope in combating the increased risk.

[7] These values are based on an internal study done by Red Alert Labs

4 EVALUATION METHODOLOGY - CONCEPT

We have defined in Chapter 2 the "What to Evaluate?" within the scope of this proposed Certification Scheme. In this Chapter we will draw the principles and concept of "How to Evaluate?" in this Certification Scheme.

The **EU IoT Device Security Certification Scheme (e-IoT-SCS)** must cover the following 3 areas within the evaluation methodology to qualify the security assurance level of an IoT Device:

1. Check that the IoT Device is conformant to its specification and covering predefined security requirements
   - For instance, at a SUBSTANTIAL level, vendors must answer a questionnaire (based on the adequate Security Profile) and provide some design evidence for the CAB to review.
2. Determinate the effectiveness of the security functionalities (Authentication, key generation, Key Management, Key storage, secure transaction, RNG, etc.) offered by the IoT device
   - For instance, at a SUBSTANTIAL level, Vulnerability scanning and Pen-testing done by a CAB with limited time and means should cover Public Vulnerabilities.
3. Check the conformance of the manufacturing and operational environments to adequate security standards (ISO 27001, IEC 62443, etc.)
   - For instance, at a SUBSTANTIAL level a simple Verification of Compliance to ISMS or SDLC standards for instance would be enough.

4.1 A Light Evaluation Methodologies

We have learned for more than 20 years from the Common Criteria (CC) Certification Scheme and made many successful moves toward improving it.

Existing approaches established by national schemes are aimed to improve and lighten the CC approach to address the market demand and procurement requirements such as:

CPA

CPA is a UK-based national scheme for commercial off-the-shelf products. It's open to all vendors, suppliers, and developers of security products whose sales base is in the UK. Since it assures security products; they are assessed against SCs (Security Characteristics) for each product type. These include web application firewalls, encryption, and smart meters. SCs also have three mitigations or requirements that each product is expected to satisfy: development, verification, and deployment.

CPA assessment is valid for two years, but since there is no mutual recognition for it, products tested in the UK won't be accepted as certified in other markets. Outside of the UK, CPA isn't widely recognized.

Baseline Security Product Assessment (BSPA)

The Dutch Baseline Security Product Assessment scheme started its pilot phase in 2015. The scheme assesses the suitability of IT security products for use in the "sensitive but unclassified" domain. It's expensive to attain, and the overall process takes up to 2 months. The average costs of certification under Baseline Security Product Assessment in the Netherlands are around 40 thousand euros.

Certification Sécuritaire de Premier Niveau (CSPN)

The National Cybersecurity Agency of France (Agence Nationale de la sécurité des systèmes d'information – ANSSI) established CSPN in 2008. It's an IT Security Certification Scheme that offers a cheaper, faster alternative to Common Criteria (CC) and Federal Information Processing Standard (FIPS) approach. CSPN is a lightweight certification process that lasts up to 8 weeks and costs between 25 thousand and 35 thousand euros. The security assurance level provided by such an evaluation is qualified to be ELEMENTARY/BASIC as per the qualification of ANSSI requirement for government ICT products procurement. This evaluation concept proved to be successful and is supported by the industry for its cost effectiveness

All of the security criteria that a product needs to meet, as well as the methodology and process of certification, are based on the standard created by the ANSSI. It only applies in France, although similar models might soon be adopted across the European Union and even the U.S

The **e-IoT-SCS** will apply the same principles with few improvements and adaptations to the IoT device types and their operational environments.

The improvements will focus on 4 main areas:

- Security Profiles based on security risk analysis which sets up security goals to be covered by an IoT device. This will add more objectiveness to the results and would allow a better comparison between products.
- Introduction of Vendor Questionnaires to replace or synthetize the Security Target and other required evidence documents.
- Enforcement of Vulnerability Scanning/Automated Tests in a way to reduce the effort on the penetration tests as much as possible. Penetration Testing could be done once during the evaluation, but the vulnerability scanning could occur early in the stage of the IoT device development life-cycle. Vendors could send results to the CAB to accelerate the testing process.
- Vulnerability Assessment Methodology to be defined specifically for IoT devices and clarify the SUBSTANTIAL level of risk scope.

4.2 Smart Platform Evaluation

Common Criteria is continuing to be improved actively within the ISO/IEC framework. CC is already a very smart approach addressing security assurance. It provides an exhaustive set of tools to elaborate a security certification process.

A very big advantage brought by the CC is its formal language used from the description of the security requirements to the evaluation methodology. This is of a great value since it leverages the objectiveness of the evaluation results by setting up a common language understood by all the stakeholders.

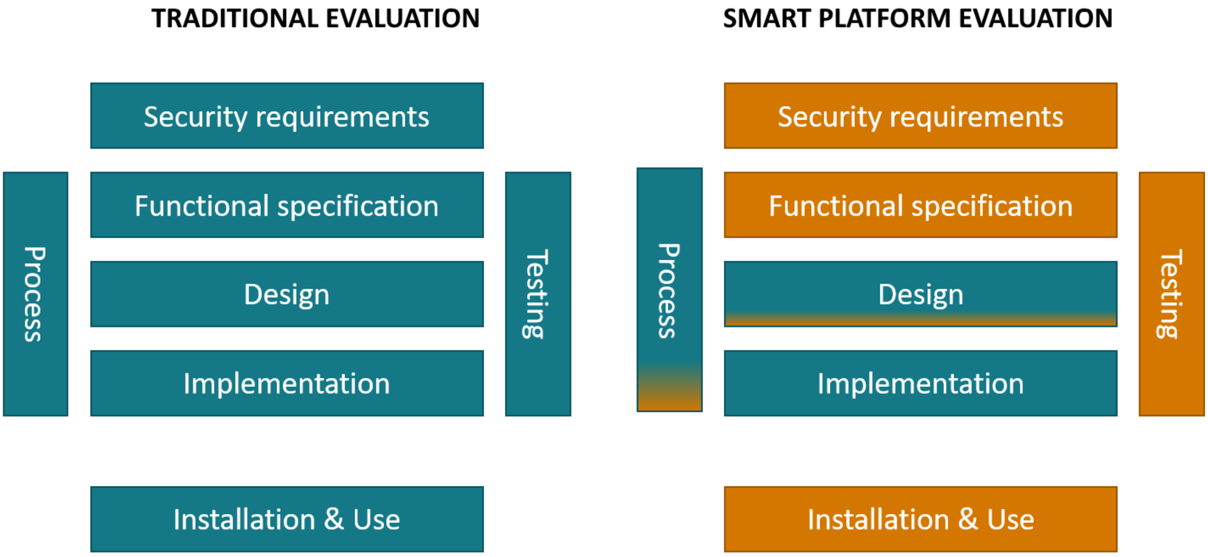
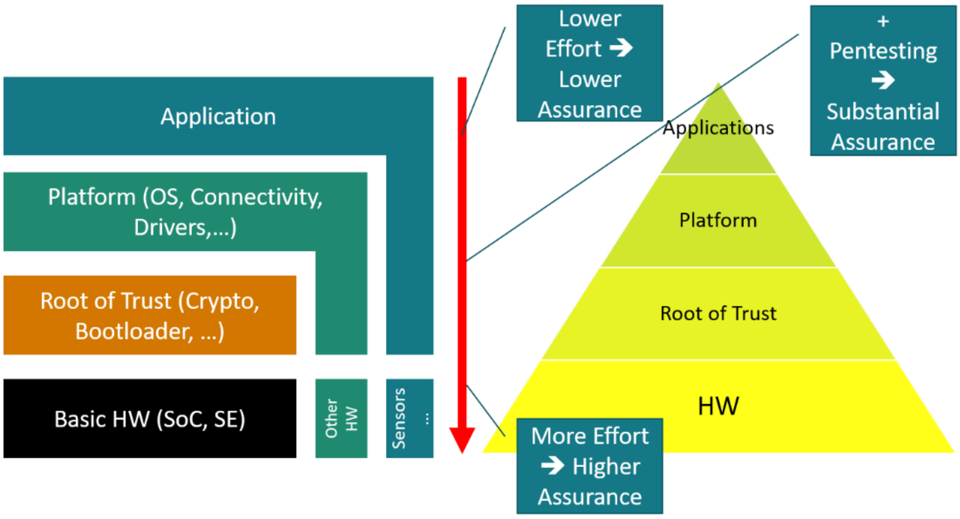


Figure 8: Smart Platform Evaluation vs Traditional Evaluation

To avoid reinventing the wheel, a Smart Platform Evaluation will be introduced to simplify certain tasks required for a traditional costly evaluation while focusing on the security testing procedures. Its goal is indeed to optimize the process by reducing the "paper" work, reduce the time required to achieve a certification while being cost-efficient. It does cover the platform which includes the Hardware, the OS and some security functionalities made available for the application layer. The composition methodology hereafter presented is a way to allow the final IoT application to be securely integrated and evaluated on the top of that platform.

4.3 Composition Methodology


Application
Platform (OS, Connectivity, Drivers,...)
Root of Trust (Crypto, Bootloader, ...)
Basic HW (SoC, SE)
Other HW
Sensors
...
Lower Effort ➔ Lower Assurance
+ Pentesting ➔ Substantial Assurance
Applications
Platform
Root of Trust
HW
More Effort ➔ Higher Assurance

The image above provides a high-level logical layer for IoT devices. On the first hand, the lower we get in the stack the lower the number of products (MCUs, MPUs, SEs) on which high security focus is required (more CC like). On the other hand, the higher in the stack the easier it should be for customers to satisfy security goals which simplifies the evaluation and certification work (can be up to self-assessment for BASIC for instance and vulnerability scanning for SUBSTANTIAL).

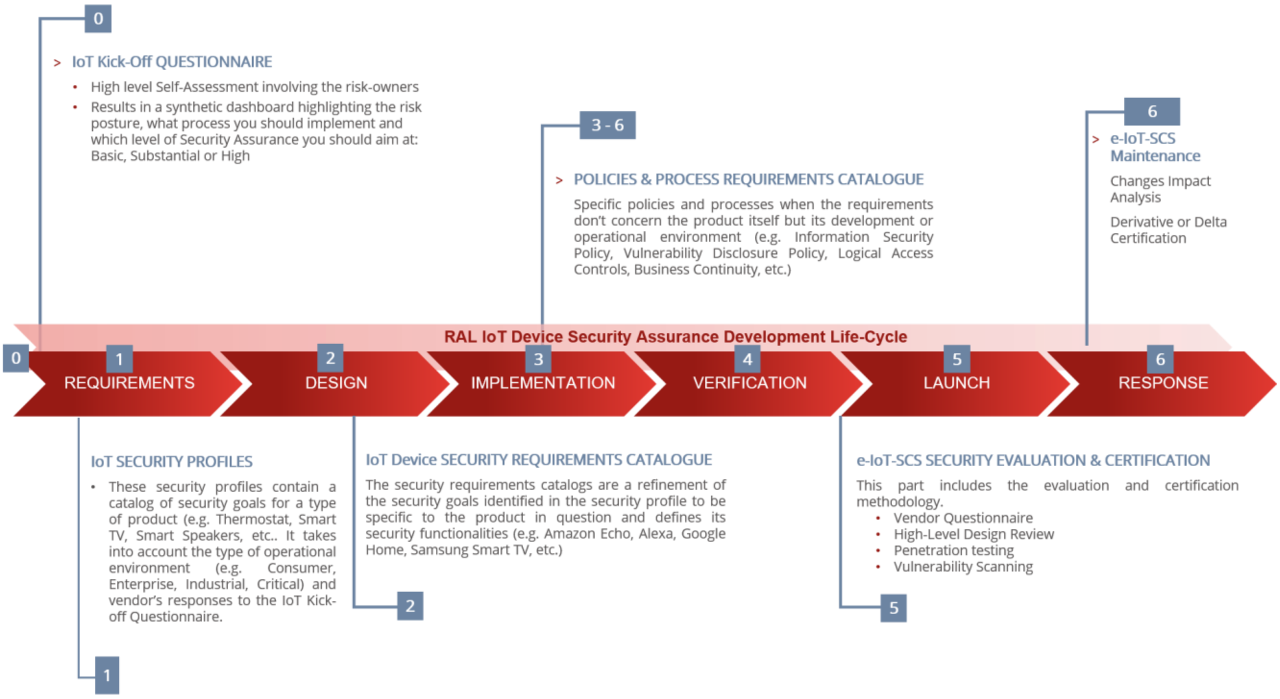
The e-IoT-SCS certification composition concept would address the following 4 scenarios:

1. Software Application on a Security Certified[8] ROE[9] (e.g. SE, TEE, TPM, Trustzone, SGX, etc.)
2. Software Application and OS Embedded on a Security Certified Hardware (e.g. IC, MCU, DSC, CM)
3. Software Application embedded on a non-Certified ROE
4. Software Application and Embedded OS on a PCB with multi-purpose Micro-Processor or an MCU Module

To provide the same level of assurance “SUBSTANTIAL” for all the 4 scenarios, the evaluation effort, time and cost would vary.

For instance, in the 1st use case, the evaluation effort is minimal (e.g. only 2 days of pentesting with vulnerability scanning) since the ROE certificate provides already a certain level of assurance whereas in the 3rd use case the evaluation requires more effort to provide the targeted level of assurance.

4.4 Integration to the IoT device Development Life-Cycle



0

> IoT Kick-Off QUESTIONNAIRE

- High level Self-Assessment involving the risk-owners
- Results in a synthetic dashboard highlighting the risk posture, what process you should implement and which level of Security Assurance you should aim at: Basic, Substantial or High

3 - 6

> POLICIES & PROCESS REQUIREMENTS CATALOGUE

Specific policies and processes when the requirements don’t concern the product itself but its development or operational environment (e.g. Information Security Policy, Vulnerability Disclosure Policy, Logical Access Controls, Business Continuity, etc.)

6

> e-IoT-SCS Maintenance

Changes Impact Analysis

Derivative or Delta Certification

1

IoT SECURITY PROFILES

- These security profiles contain a catalog of security goals for a type of product (e.g. Thermostat, Smart TV, Smart Speakers, etc.. It takes into account the type of operational environment (e.g. Consumer, Enterprise, Industrial, Critical) and vendor’s responses to the IoT Kick-off Questionnaire.

2

IoT Device SECURITY REQUIREMENTS CATALOGUE

The security requirements catalogs are a refinement of the security goals identified in the security profile to be specific to the product in question and defines its security functionalities (e.g. Amazon Echo, Alexa, Google Home, Samsung Smart TV, etc.)

5

e-IoT-SCS SECURITY EVALUATION & CERTIFICATION

This part includes the evaluation and certification methodology.

- Vendor Questionnaire
- High-Level Design Review
- Penetration testing
- Vulnerability Scanning

Figure 9: RAL IoT Device Security Assurance Development Life-Cycle[10]

4.5 Concept of Relationship to Other Relevant Certification Schemes

It is obvious that some of the vendors had gone (or will go) through other certification schemes tailored to the IoT Device. This could be related to the scope of their addressable market or for legacy reasons.

The e-IoT-SCS approach is not intended to reinvent the wheel but to allow reusing other certification schemes evidence and results. Indeed, the formalism used is not the focus of this methodology.

[8] CC like evaluation

[9] Restricted Operating Environment

[10] This approach has been developed and tested efficiently by Red Alert Labs

Vendors would have to make sure that their evidence (documentation, tests, etc.) are oriented by security functionality and not by functional design.

These relationships could be defined with the most common private/public schemes internationally allowing vendors to reduce costs and time on re-certifications (when required).

• The mapping table concept

A mapping table could be requested in case a vendor reuses existing certification evidence. This mapping table will address the Vendor Questionnaires on the first column, the area of evidence (ADV, ATE, ASE, etc.) it belongs too, the Vendor Proposed evidence/document fulfilling the requirement and a final column for Rationale.

Questionnaire	Category	Provided Evidence	Rationale
The Vendor must provide an explicit description of the TOE logical and Physical boundary.	ASE / Documentation	Security Target Section 2.1 or Security Policy Section 1.2 or .ppt file attached, etc.	Our TOE is an IoT Device which is composed of a software application embedded on PCB with a hard case. Please find more details about the boundary in the provided evidence.

• Reuse of Other Certification Schemes

Let’s try to identify a potential relationship to the ISA 62443 EDSA and SDLA Certification Scheme.

The ISA 62443 EDSA (Embedded Device Security Assurance) certification program offers a set of devices a process requirement. An embedded device meeting such requirements can be granted the ISASecure Symbol/Label. Whereas the SDLA (Security Development Lifecycle Assurance) certification program which defines the requirements to certify a supplier’s development lifecycle process.

EDSA scheme allows 3 level of assurance (SL1 to SL3) covering 3 parts:

1. Security Development Assessment
2. Functional Security Assessment
3. Robustness Testing (Vulnerability Identification Testing + Communication Robustness Testing)

We expect to provide at later stage in the definition of the e-IoT-SCS scheme a mapping table between the requirements covering the 3 parts above and the e-IoT-SCS requirements. This will help in identifying the delta/gaps (if any) and address them “only” during the certification.

Same goes for the SDLA, which is in line with the Development Life-Cycle integration as described in Section 4.4 above.

4.6 Expected results

The e-IoT-SCS Evaluation Report will be issued by CABs and will mostly be based on a template simplifying and harmonizing the work. This will provide end users and device suppliers with the right type of information summarizing the work done the results of the assessment.

A trademark/label could be created for customer assurance and marketing purposes. This label should attest the presence of a successful certification and should reference the evaluation report which could be consulted for more information.

Note that those expected results must be reusable in between stakeholders which requires these to be structured in a specific way allowing the editor to extract "non-shareable" information.

4.7 Delta & Derivative Certification Concepts

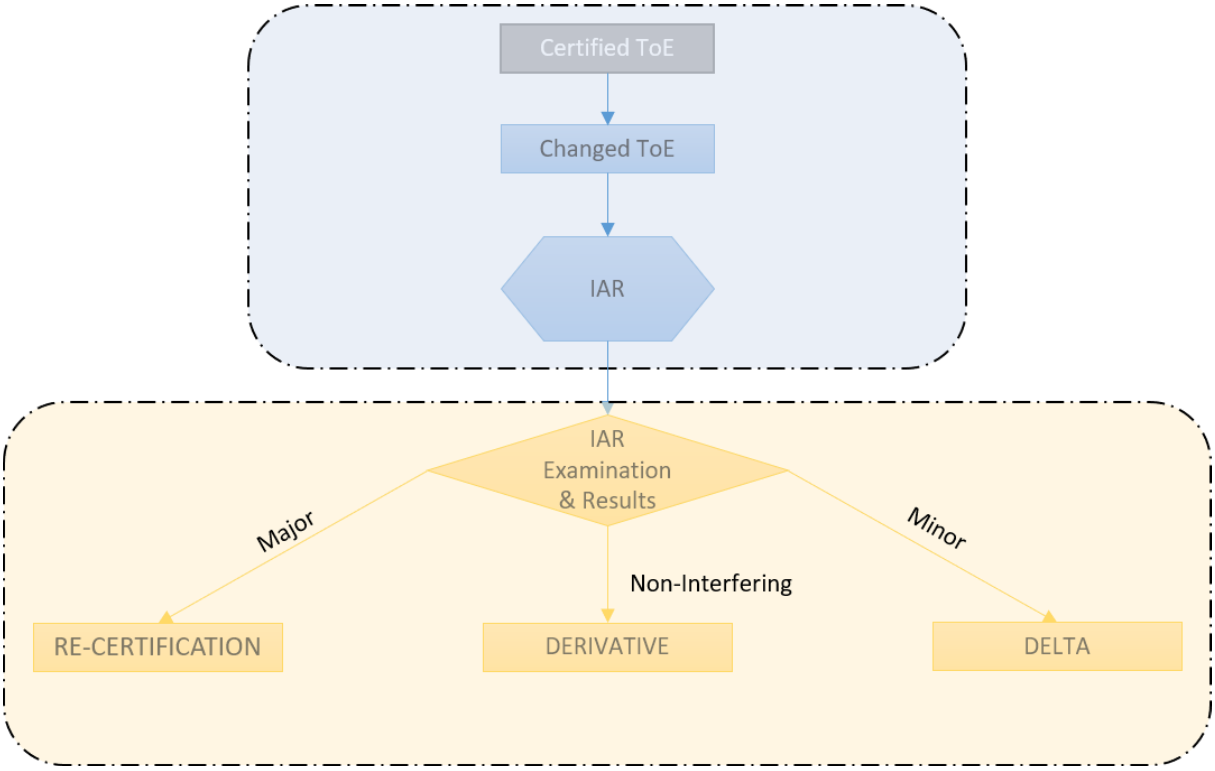


Figure 10: Impact Analysis Report - Delta & Derivative Concepts

The Delta & Derivative Certification are intended to simplify the maintenance of the certificate and minimize the costs when certifying a family of IoT devices. The criteria will be defined clearly allowing when it is possible a straightforward judgement on the nature of the changes. A "Major" change will require a full recertification, a "Non-Interfering (with the security requirements)" change will be required only a new stamp and a "Minor" change will require a Delta certification relying on existing artefacts.

This process will consider the vendor's proven capabilities in processing vulnerability disclosure, upgrades and incident response. An Impact Assessment Process on the manufacturing side could simplify this task.

4.8 Certification Maintenance Procedures

Millions of IoT devices are expected to be granted certifications. These certifications must be maintained in a proper and cost efficient to guarantee the level of assurance and the validity of the certificate in the operational phase.

Certification must be maintained for the following 3 reasons:

1. A vulnerability related to the ToE was disclosed

2. The Security Goals and Requirements defined in the relevant Security Profile had a major change
3. The vendor has updated the ToE with a Minor Change

The metadata certification concept is intended to provide an attestation for each certified IoT device. This concept will allow service providers, vendors and users to attest the validity of the certificate. Service providers would be able to impose security policies relying on the metadata statements that are provided by the manufacturer.

4.9 Evaluation Cost Estimation

The following estimation is not based on statistical data but is based on the market expectations. It considers the technical and commercial constraints imposed in IoT. The scope in perspective being the application layer only while considering a composite evaluation on a smart underlying platform.

Security Functions (sample)	Scope	Elapsed Time of Evaluation	Expertise (in Days)	Depth of Evaluation [11]	Cost
IP Protection **Data Privacy**	Consumer (Basic)	1-2 weeks	1-5 days	Black-Box/ Self-Assessment	1K€ to 5K€
Strong Authentication **Strong Encryption** **Data Confidentiality** **IP Protection** **Data Availability** **Data Privacy**	Enterprise (Basic to Substantial)	2-3 weeks	5-10 days	Black-box to Grey-box	5K€ to 10K€
Strong Authentication **Communication Integrity** **Strong Encryption** **Data Confidentiality** **IP Protection** **Data Availability** **Data Privacy** **Human Safety**	Industrial (Substantial to High)	3-4 weeks	10-15 days	Grey-Box to White-Box	10K€ to 15K€
Strong Authentication	Critical (High)	4-6 weeks	15-20 days	White-Box	15K€ to 20K€

[11] With a focus on vulnerability scanning and/or pentesting

Firmware Integrity **Communication Integrity** **Strong Encryption** **Data Confidentiality** **IP Protection** **Data Availability** **Data Privacy** **Human Safety** **Tamper Resistant**					

4.10 Potential Pilot Project

A pilot project will be defined at the 2nd Phase – Beta version of the Candidate Certification Scheme. This will involve volunteered companies and will result in a report and list of action to update the candidate scheme accordingly.

5 IMPLEMENTATION PLANNING

5.1 Components/Deliverables

1. Certification Scheme Policy: Document defining the policies and processes that govern the IoT device certification program
2. Certification Evaluation Methodology: Document defining the review and test procedures from A to Z
3. General Protection Profile: The main output of this document will be a list of security goals/objectives qualifying the need to counter threats identified on a typical IoT device
4. Guidelines- CABs Evaluation & Certification Agreement: Document listing the rules of agreement between CABs and Certification Scheme stakeholders
5. Guidelines- CABs Accreditation Policy: Document describing the process for CABs accreditation
6. Vulnerability Disclosure, Patching & Assurance Maintenance Policy: Document describing the life-cycle management of the Certificate after issuance
7. Label Policy: Document describing the Labelisation policy
8. The Metadata Certification Policy: Document describing the Metadata Certification Concept and Requirements guaranteeing the relevancy and Authenticity of the Certificates.
9. Templates (Vendor Questionnaire, Impact Analysis Report, Security Profile, Evaluation Report, Mapping Table Concept)

5.2 Estimated Timeline

Version	Description	Delivery Date
Pre-Study	This covers the current version of the document which sets the common understanding and principles to follow while developing the certification scheme candidate	1st of October, 2018
Prototype	This is a first version covering the first 3 documents listed above which are the basis of the certification scheme policy and evaluation methodology.	31st of December, 2018
Beta	This version will include the rest of the deliverables listed above. The prototype version will be updated with the first return on experience from a potential pilot project.	29th of March, 2019

ANNEX II – SECURITY IMPACT CALCULATION - RESEARCH

BSI IMPACT GRID

Considers impact based on the effect of loss of confidentiality, integrity, or availability on a process, application or data.

NORMAL: The impact of any loss or damage is limited and calculable.

HIGH: The impact of any loss or damage may be considerable

VERY HIGH: The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival of the organization.

	NORMAL	HIGH	VERYHIGH
Violations of laws, regulations, or contracts	Violations of regulations and laws with minor consequences Minor breaches of contract which result in at most minor contractual penalties	Violations of regulations and laws with substantial consequences Major breaches of contract with high contractual penalties	Fundamental violations of regulations and laws Breaches of contract with ruinous damage liabilities
Impairment of the right to informational self-determination	This deals with personal data whose processing could adversely affect the social standing or financial well-being of those concerned.	This aspect deals with personal data whose processing could have a seriously adverse effect on the social standing or financial well-being of those concerned.	This aspect deals with personal data whose processing could result in the injury or death of the persons concerned or that could endanger the personal freedom of the persons concerned.
Physical injury	Does not appear possible.	Physical injury to an individual cannot be absolutely ruled out.	Serious injury to an individual is possible. There is a danger to life and limb.
Impaired ability to perform the tasks at hand	Impairment was assessed to be tolerable by those concerned. The maximum acceptable downtime is greater than 24 hours.	Impairment of the ability to perform the tasks at hand was assessed as intolerable by some of the individuals concerned.	Impairment of the ability to perform tasks was assessed as intolerable by all individuals concerned.

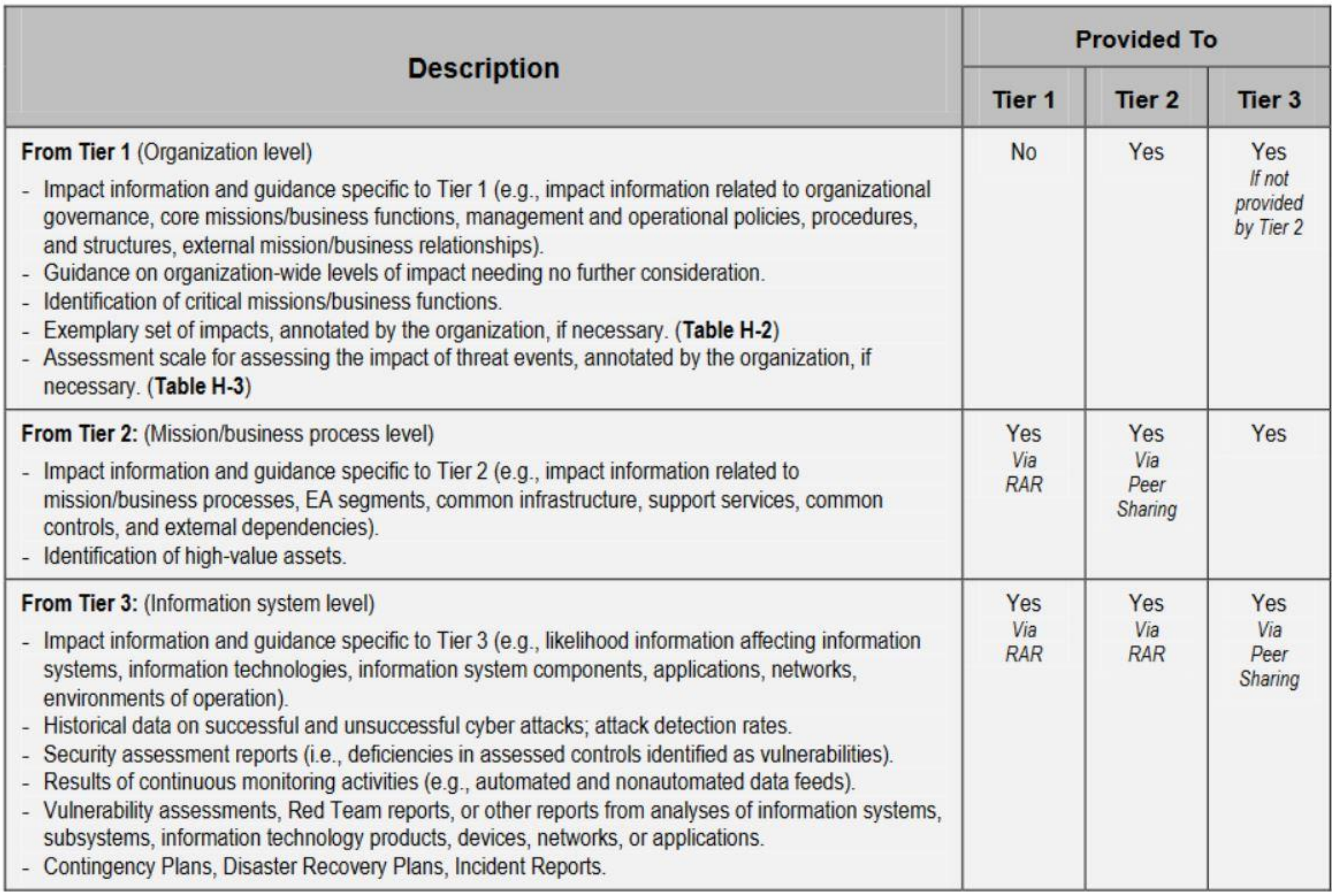
		The maximum acceptable down time is between one and 24 hours.	The maximum acceptable down time is less than one hour.
Negative internal or external effects	Only minimal impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.	Considerable impairment of the reputation / trustworthiness can be expected	A nation-wide or state-wide loss of reputation / trustworthiness is conceivable, possibly even endangering the existence of the Organisation.
Financial consequences	The financial loss is acceptable to the organisation	The financial loss is considerable but does not threaten the existence of the organisation.	The financial loss threatens the existence of the organisation.

BSI Paradigm for determining protection requirements for IT systems.

1. The damage event or total damage with the most serious consequences determine the protection requirements of an IT system **(maximum principle).**
2. When examining the possible damage and its consequences, it must also be kept in mind that the applications may use the results of other applications as input. **(accounting for dependencies)**.
3. If several applications or a lot of information is processed on an IT system, then you must determine if the accumulation of several (e.g. smaller) damage events on one IT system could result in a higher amount of total damage. In this case, the protection requirements of the IT system increase accordingly **(cumulative effect)**.
4. The opposite effect can also occur. This means it is possible for an application to have high protection requirements, but its protection requirements are not assigned to the IT system being examined because only minor parts of the application run on that IT system. In this case, the protection requirements must be reallocated **(distribution effect)**

NIST METHODOLOGY

TABLE H-1: INPUTS – DETERMINATION OF IMPACT



Description	Provided To		
	Tier 1	Tier 2	Tier 3
From Tier 1 (Organization level) - Impact information and guidance specific to Tier 1 (e.g., impact information related to organizational governance, core missions/business functions, management and operational policies, procedures, and structures, external mission/business relationships). - Guidance on organization-wide levels of impact needing no further consideration. - Identification of critical missions/business functions. - Exemplary set of impacts, annotated by the organization, if necessary. (**Table H-2**) - Assessment scale for assessing the impact of threat events, annotated by the organization, if necessary. (**Table H-3**)	No	Yes	Yes *If not provided by Tier 2*
From Tier 2: (Mission/business process level) - Impact information and guidance specific to Tier 2 (e.g., impact information related to mission/business processes, EA segments, common infrastructure, support services, common controls, and external dependencies). - Identification of high-value assets.	Yes *Via RAR*	Yes *Via Peer Sharing*	Yes
From Tier 3: (Information system level) - Impact information and guidance specific to Tier 3 (e.g., likelihood information affecting information systems, information technologies, information system components, applications, networks, environments of operation). - Historical data on successful and unsuccessful cyber attacks; attack detection rates. - Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities). - Results of continuous monitoring activities (e.g., automated and nonautomated data feeds). - Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications. - Contingency Plans, Disaster Recovery Plans, Incident Reports.	Yes *Via RAR*	Yes *Via RAR*	Yes *Via Peer Sharing*

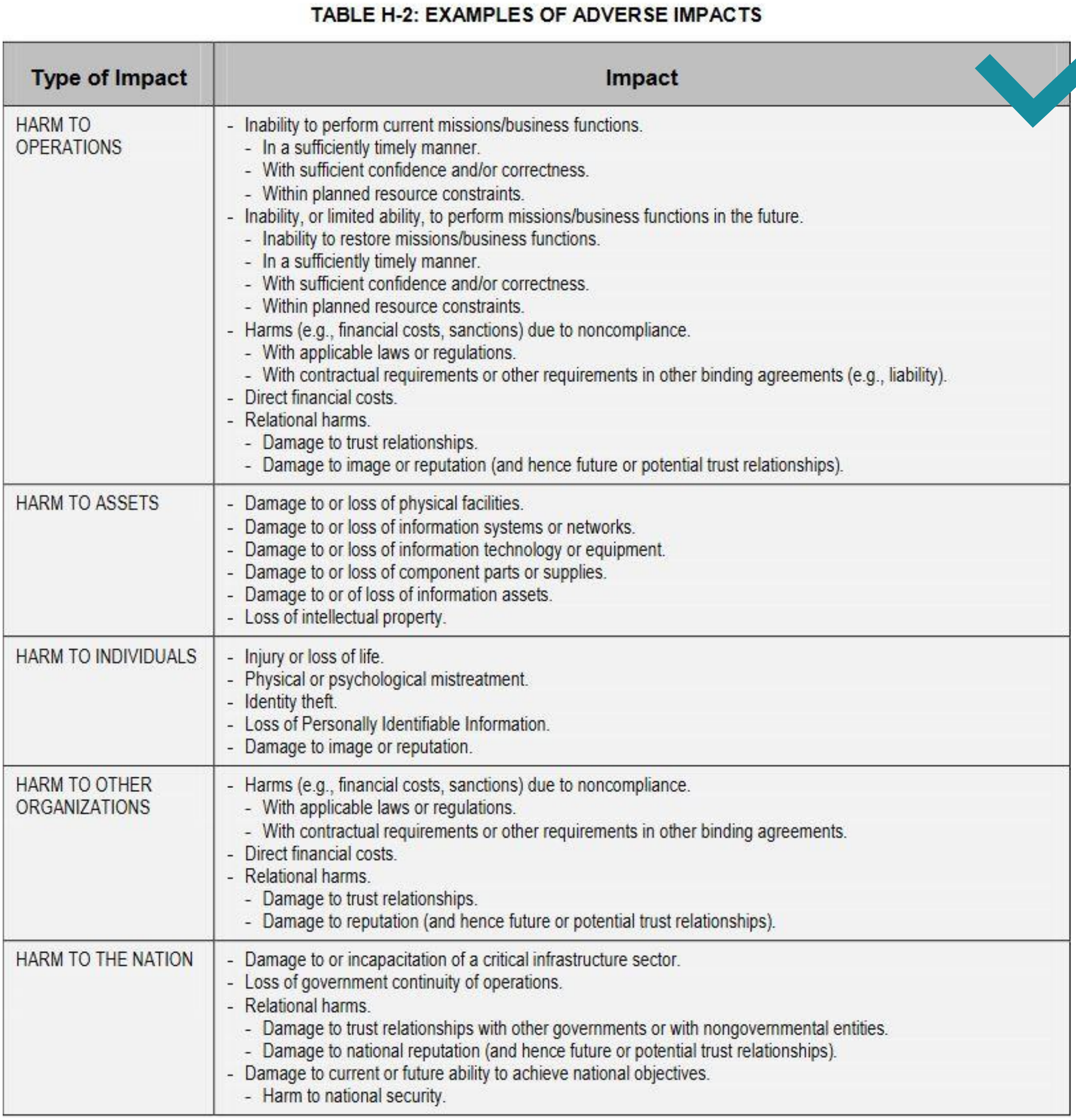
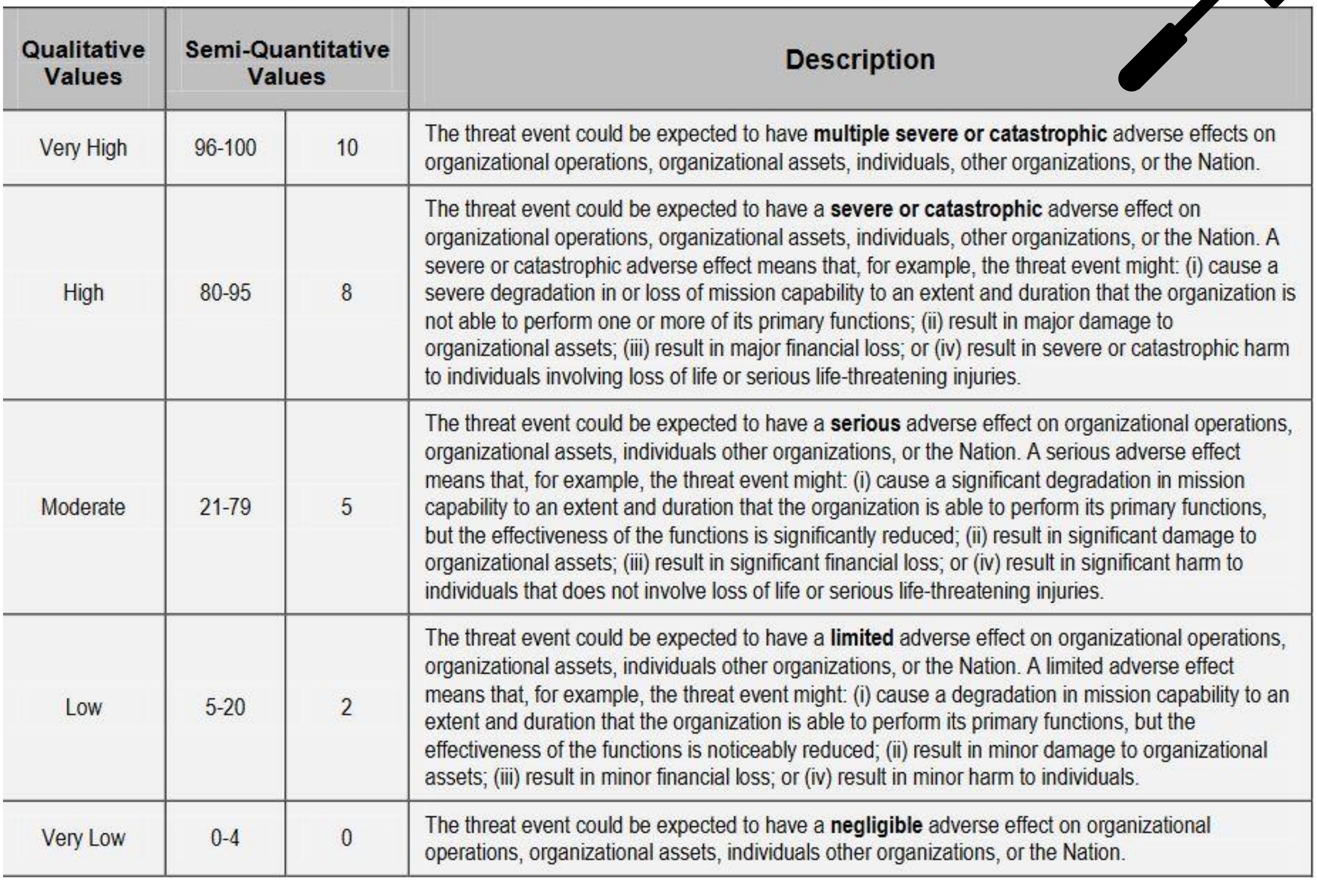


TABLE H-2: EXAMPLES OF ADVERSE IMPACTS

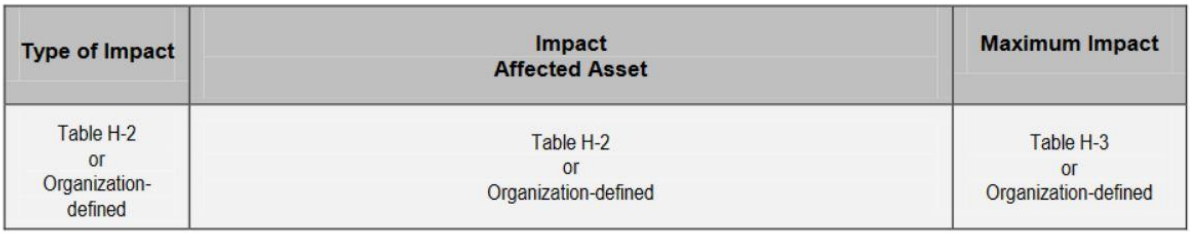
Type of Impact	Impact
HARM TO OPERATIONS	- Inability to perform current missions/business functions. - In a sufficiently timely manner. - With sufficient confidence and/or correctness. - Within planned resource constraints. - Inability, or limited ability, to perform missions/business functions in the future. - Inability to restore missions/business functions. - In a sufficiently timely manner. - With sufficient confidence and/or correctness. - Within planned resource constraints. - Harms (e.g., financial costs, sanctions) due to noncompliance. - With applicable laws or regulations. - With contractual requirements or other requirements in other binding agreements (e.g., liability). - Direct financial costs. - Relational harms. - Damage to trust relationships. - Damage to image or reputation (and hence future or potential trust relationships).
HARM TO ASSETS	- Damage to or loss of physical facilities. - Damage to or loss of information systems or networks. - Damage to or loss of information technology or equipment. - Damage to or loss of component parts or supplies. - Damage to or of loss of information assets. - Loss of intellectual property.
HARM TO INDIVIDUALS	- Injury or loss of life. - Physical or psychological mistreatment. - Identity theft. - Loss of Personally Identifiable Information. - Damage to image or reputation.
HARM TO OTHER ORGANIZATIONS	- Harms (e.g., financial costs, sanctions) due to noncompliance. - With applicable laws or regulations. - With contractual requirements or other requirements in other binding agreements. - Direct financial costs. - Relational harms. - Damage to trust relationships. - Damage to reputation (and hence future or potential trust relationships).
HARM TO THE NATION	- Damage to or incapacitation of a critical infrastructure sector. - Loss of government continuity of operations. - Relational harms. - Damage to trust relationships with other governments or with nongovernmental entities. - Damage to national reputation (and hence future or potential trust relationships). - Damage to current or future ability to achieve national objectives. - Harm to national security.

TABLE H-3: ASSESSMENT SCALE – IMPACT OF THREAT EVENTS



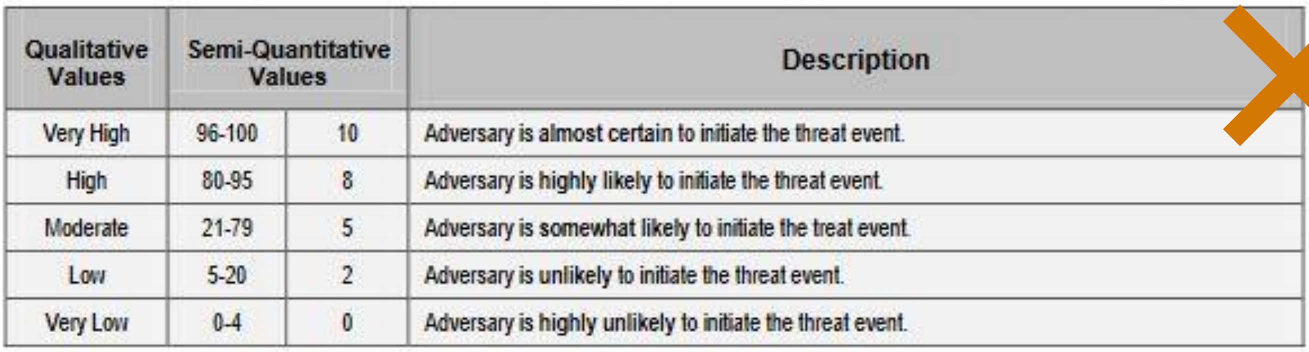
Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS



Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Table H-3 or Organization-defined

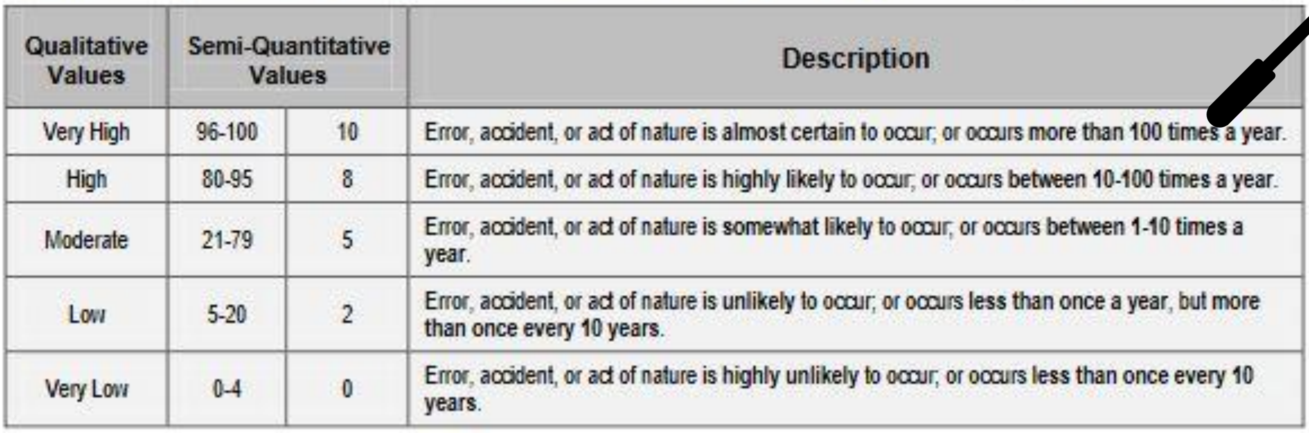
TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)



✗

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is almost certain to initiate the threat event.
High	80-95	8	Adversary is highly likely to initiate the threat event.
Moderate	21-79	5	Adversary is somewhat likely to initiate the treat event.
Low	5-20	2	Adversary is unlikely to initiate the threat event.
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event.

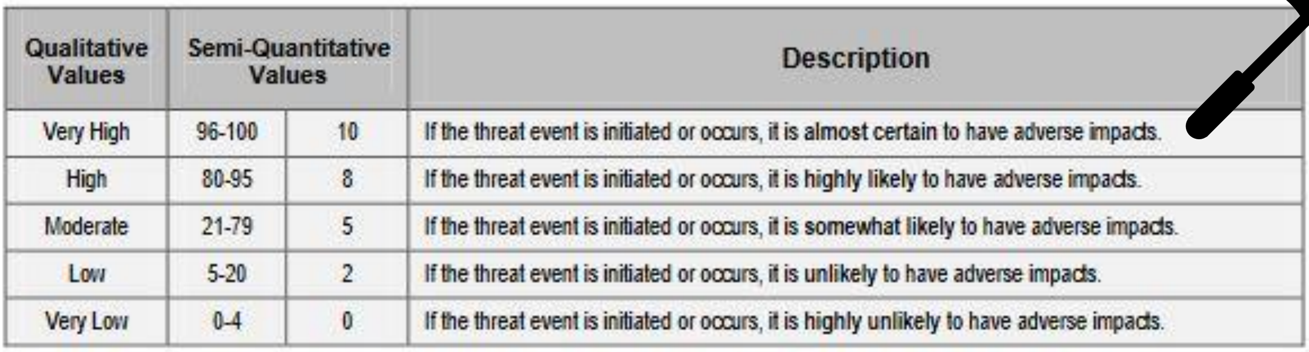
TABLE G-3: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT OCCURRENCE (NON-ADVERSARIAL)



🔨

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	80-95	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	5-20	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

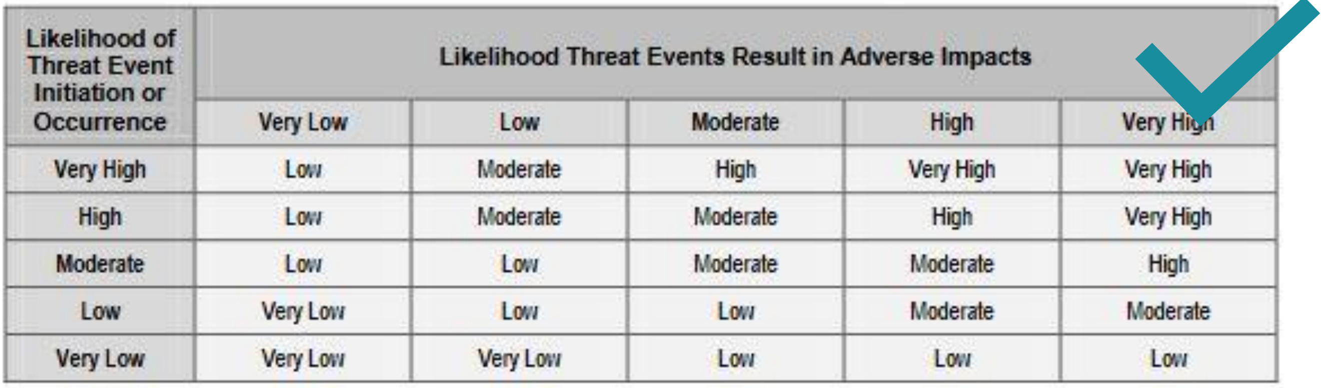
TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS



🔨

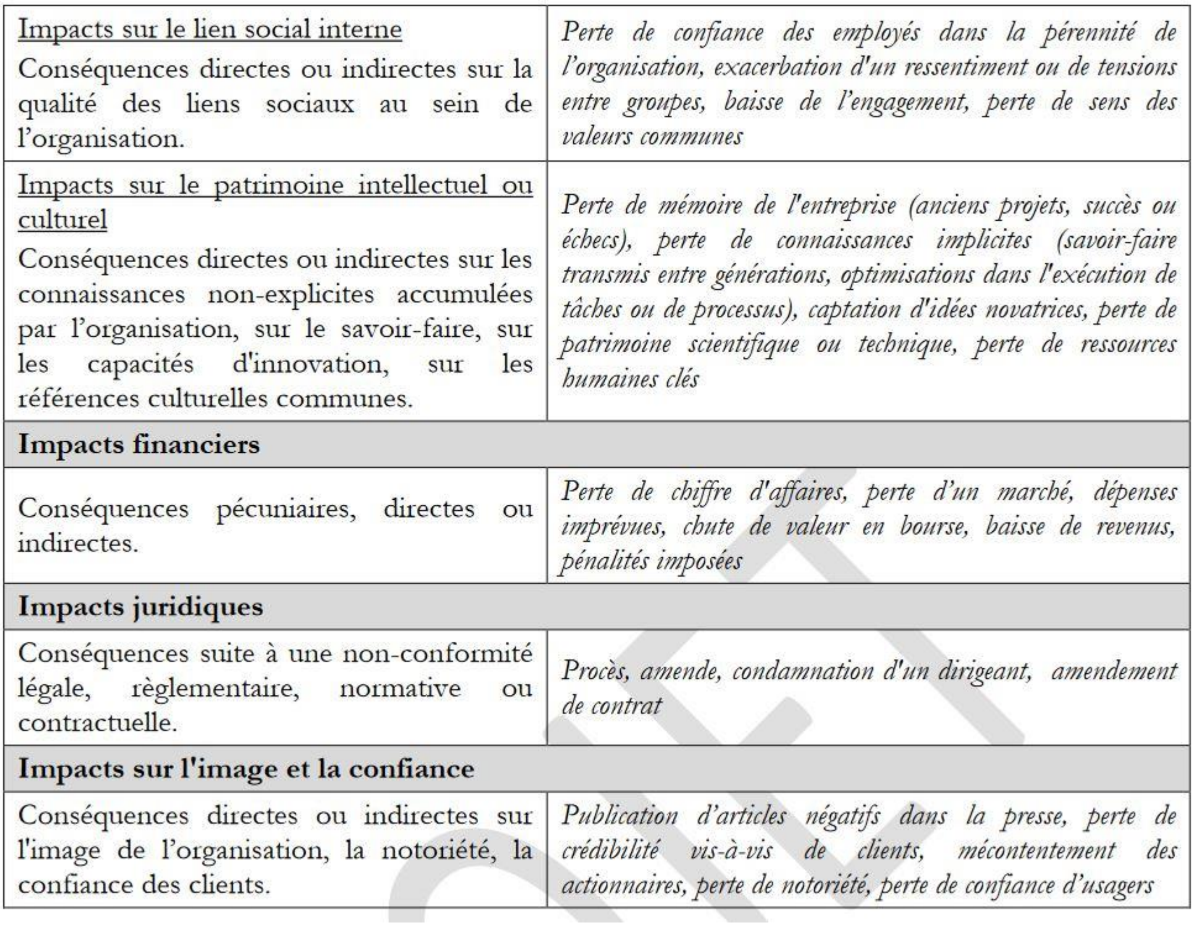
Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

TABLE G-5: ASSESSMENT SCALE – OVERALL LIKELIHOOD

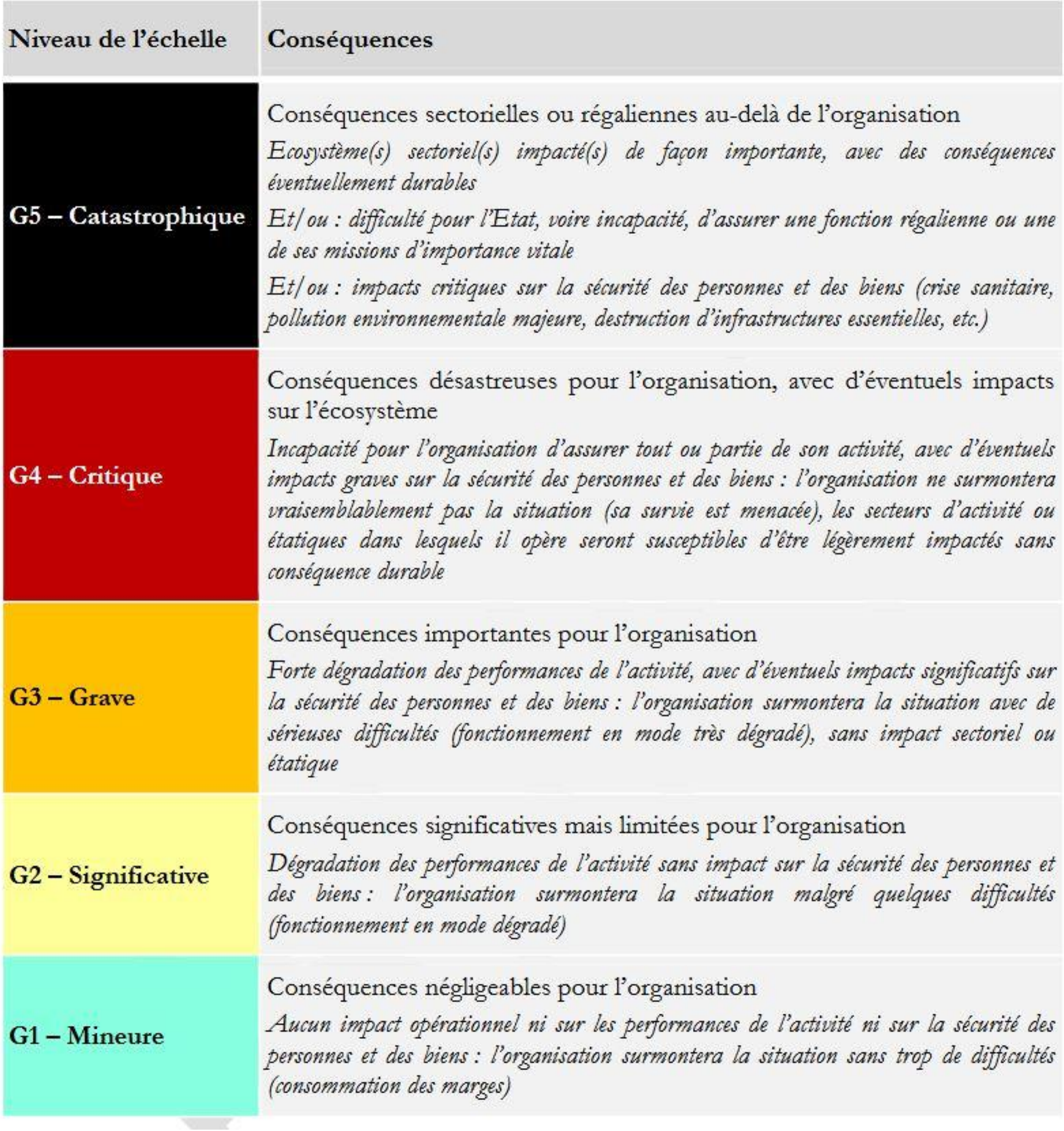


✓

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low



Impacts sur le lien social interne Conséquences directes ou indirectes sur la qualité des liens sociaux au sein de l'organisation.	*Perte de confiance des employés dans la pérennité de l'organisation, exacerbation d'un ressentiment ou de tensions entre groupes, baisse de l'engagement, perte de sens des valeurs communes*
Impacts sur le patrimoine intellectuel ou culturel Conséquences directes ou indirectes sur les connaissances non-explicites accumulées par l'organisation, sur le savoir-faire, sur les capacités d'innovation, sur les références culturelles communes.	*Perte de mémoire de l'entreprise (anciens projets, succès ou échecs), perte de connaissances implicites (savoir-faire transmis entre générations, optimisations dans l'exécution de tâches ou de processus), captation d'idées novatrices, perte de patrimoine scientifique ou technique, perte de ressources humaines clés*
Impacts financiers	
Conséquences pécuniaires, directes ou indirectes.	*Perte de chiffre d'affaires, perte d'un marché, dépenses imprévues, chute de valeur en bourse, baisse de revenus, pénalités imposées*
Impacts juridiques	
Conséquences suite à une non-conformité légale, règlementaire, normative ou contractuelle.	*Procès, amende, condamnation d'un dirigeant, amendement de contrat*
Impacts sur l'image et la confiance	
Conséquences directes ou indirectes sur l'image de l'organisation, la notoriété, la confiance des clients.	*Publication d'articles négatifs dans la presse, perte de crédibilité vis-à-vis de clients, mécontentement des actionnaires, perte de notoriété, perte de confiance d'usagers*



Niveau de l'échelle	Conséquences
G5 – Catastrophique	Conséquences sectorielles ou régaliennes au-delà de l'organisation *Ecosystème(s) sectoriel(s) impacté(s) de façon importante, avec des conséquences éventuellement durables* *Et/ou : difficulté pour l'Etat, voire incapacité, d'assurer une fonction régalienne ou une de ses missions d'importance vitale* *Et/ou : impacts critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale majeure, destruction d'infrastructures essentielles, etc.)*
G4 – Critique	Conséquences désastreuses pour l'organisation, avec d'éventuels impacts sur l'écosystème *Incapacité pour l'organisation d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens : l'organisation ne surmontera vraisemblablement pas la situation (sa survie est menacée), les secteurs d'activité ou étatiques dans lesquels il opère seront susceptibles d'être légèrement impactés sans conséquence durable*
G3 – Grave	Conséquences importantes pour l'organisation *Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens : l'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans impact sectoriel ou étatique*
G2 – Significative	Conséquences significatives mais limitées pour l'organisation *Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens : l'organisation surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)*
G1 – Mineure	Conséquences négligeables pour l'organisation *Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens : l'organisation surmontera la situation sans trop de difficultés (consommation des marges)*

ANNEX III – RISK MANAGEMENT METHODOLOGY

EBIOS RISK MANAGEMENT

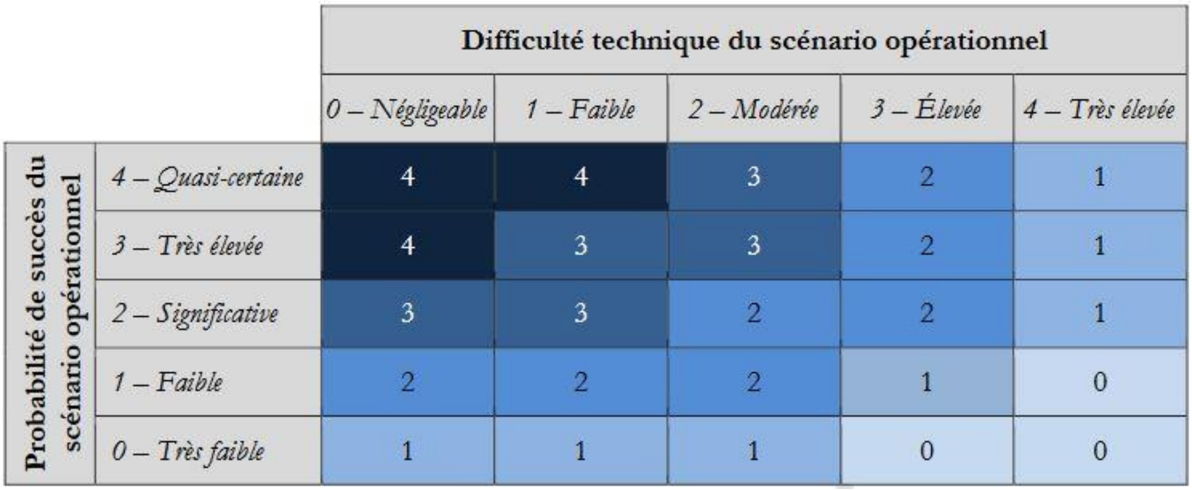
Assess the Likelihood

According to EBIOS methodology, we prepare an attacker's graph first. This is made once we study the four steps, from the perspective of an attacker, that how he can execute his actions. The four steps are Understand (e.g.: Social engineering), Enter (e.g.: Intrusion), Find and Exploit. Then we proceed to the evaluation of its likelihood. The likelihood levels can be 5, like the case of Impacts scale. These levels are Almost-certain, Very likely, Likely, Little likely and Unlikely. These all depends upon the chances of the risk sources to attain its objective (i.e. to attack). According to EBIOS, there are three approaches to choose the operational scenario for this. They are Express method, Standard method and Advanced method.

Express method (direct quotation of the overall likelihood of the scenario):

The express method consists of directly evaluating the overall likelihood of the scenario, based on general considerations relative to the source of risk (motivations, resources, determination and capacity/competence) and the security of supporting assets targeted in the scenario (exposure, vulnerabilities).

In this approach, you can either directly estimate the likelihood level of the scenario to score its probability of success and its technical difficulty and deduce by crossing the likelihood of the scenario according to the standard matrix presented here:



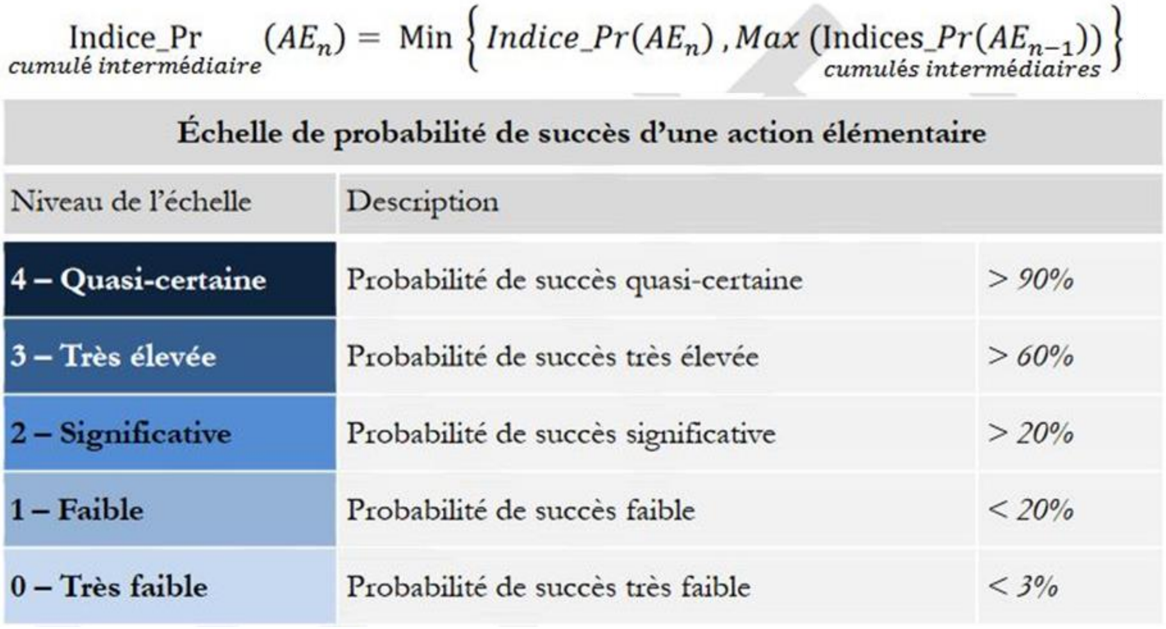
		Difficulté technique du scénario opérationnel				
		0 – Négligeable	*1 – Faible*	*2 – Modérée*	*3 – Élevée*	*4 – Très élevée*
Probabilité de succès du scénario opérationnel	*4 – Quasi-certaine*	4	4	3	2	1
	3 – Très élevée	4	3	3	2	1
	2 – Significative	3	3	2	2	1
	1 – Faible	2	2	2	1	0
	0 – Très faible	1	1	1	0	0

The mapping is made between the probability of success of operational scenario and the technical difficulty of the operational scenario.

Standard method (probability of success of elementary actions):

In the standard method you will rate each elementary action according to an index of probability of success seen from the attacker's perspective. The following scale can be adopted, the percentages are mentioned as an indication to facilitate the listing.

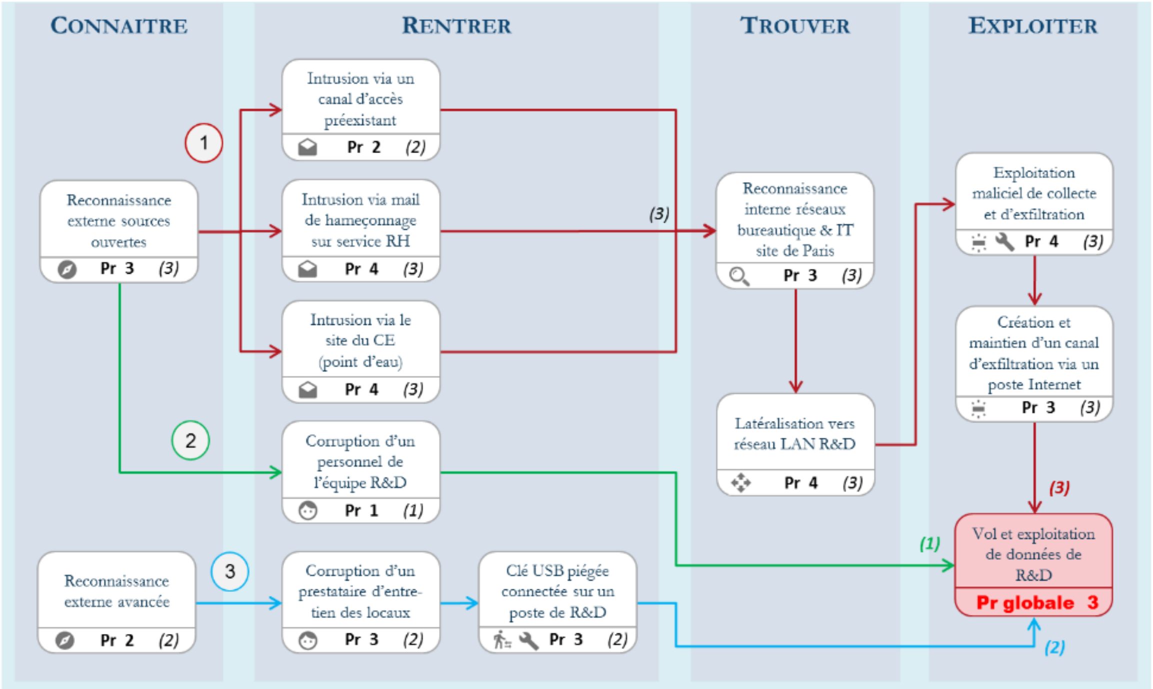
You have scored in the previous step each elementary action according to a probability index of success. You can evaluate the overall index of probability of success scenario by applying the following rule. The principle is to progress in a procedure by evaluating step by step each elementary action "AE_n" of a node "n", an intermediate cumulative probability index from the elementary index of "AE_n" And intermediate cumulative indices of the previous node "n-1".



$$\underset{cumul\acute{e}\ interm\acute{e}diaire}{\text{Indice\_Pr}}(AE_n) = \text{Min}\left\{Indice\_Pr(AE_n)\,, Max\,\Big(\underset{cumul\acute{e}s\ interm\acute{e}diaires}{\text{Indices\_}Pr(AE_{n-1})}\Big)\right\}$$

Échelle de probabilité de succès d'une action élémentaire		
Niveau de l'échelle	Description	
4 – Quasi-certaine	Probabilité de succès quasi-certaine	*> 90%*
3 – Très élevée	Probabilité de succès très élevée	*> 60%*
2 – Significative	Probabilité de succès significative	*> 20%*
1 – Faible	Probabilité de succès faible	*< 20%*
0 – Très faible	Probabilité de succès très faible	*< 3%*

Let us consider an example of e-mail phishing, which has an index of '3- Very high'. Here the probability of the attacker to succeed in his action depends on the chances that the employee or the targeted person clicks on the malicious attachment.


CONNAITRE
RENTRER
TROUVER
EXPLOITER
1
2
3
Reconnaissance externe sources ouvertes
Pr 3 (3)
Reconnaissance externe avancée
Pr 2 (2)
Intrusion via un canal d'accès préexistant
Pr 2 (2)
Intrusion via mail de hameçonnage sur service RH
Pr 4 (3)
Intrusion via le site du CE (point d'eau)
Pr 4 (3)
Corruption d'un personnel de l'équipe R&D
Pr 1 (1)
Corruption d'un prestataire d'entretien des locaux
Pr 3 (2)
Clé USB piégée connectée sur un poste de R&D
Pr 3 (2)
(3)
Reconnaissance interne réseaux bureautique & IT site de Paris
Pr 3 (3)
Latéralisation vers réseau LAN R&D
Pr 4 (3)
Exploitation maliciel de collecte et d'exfiltration
Pr 4 (3)
Création et maintien d'un canal d'exfiltration via un poste Internet
Pr 3 (3)
(3)
(1)
(2)
Vol et exploitation de données de R&D
Pr globale 3

Let us plot an example where we can illustrate from an attacker's perspective, the three modes of operation he performs in order to find out the probability of each modes. After acquiring some knowledge about the external sources which are open (Probability Pr 3), the attacker can enter into the system in two main different ways. The first one indicated in red coloured (number 1, which has three elementary actions) and the second one indicated in green colour 2. There is a third way (blue coloured 3) which is based on the advanced external knowledge (Probability Pr 2). The probability of each elementary action 'AE' is calculated according to the equation above.

For example calculating the probability of first node under "Trouver",

Indice_Pr ($AE_{Pr\ 3}$) = Min {Indice_Pr($AE_{Pr\ 3)}$, Max(Indices_Pr($AE_{Pr\ 2}$, $AE_{Pr\ 4}$, AE_{Pr4}))}
= Min {3, Max (2,3,3)}
= Min {3,3}
= 3

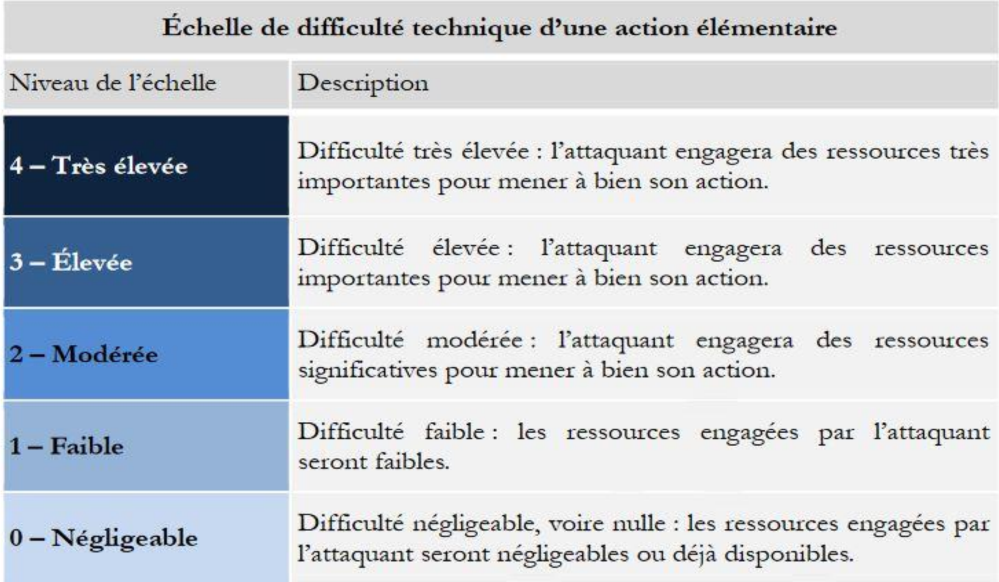
Like this, we calculate for each nodes (AE). And obtain a final probability value for each path. The value for the first path being "3", the second path being "1" and the third path being "2".

The global index of likelihood of success of the scenario is estimated to "3-Very high": the achievement of the purpose of the source of the risk according to one or the other Operational modes of the scenario operational is considered as **Very likely (V3)**. The operating mode the easiest or feasible being the red number 1.

Advanced method (probability of success and technical difficulty of the Elementary actions):

In the advanced method, you will also rate the technical difficulty of achieving the elementary action, from the point of view of the attacker. It allows to estimate the resources that the attacker will have to engage to carry out his action and increase his chances of success. The scale following may be adopted:

$$\underset{\textit{cumulé intermédiaire}}{\text{Indice\_Diff}}(AE_n) = \text{Max}\left\{ Indice\_Diff(AE_n)\,, Min\,(\underset{\textit{cumulés intermédiaires}}{\text{Indices\_}Diff}(AE_{n-1})) \right\}$$

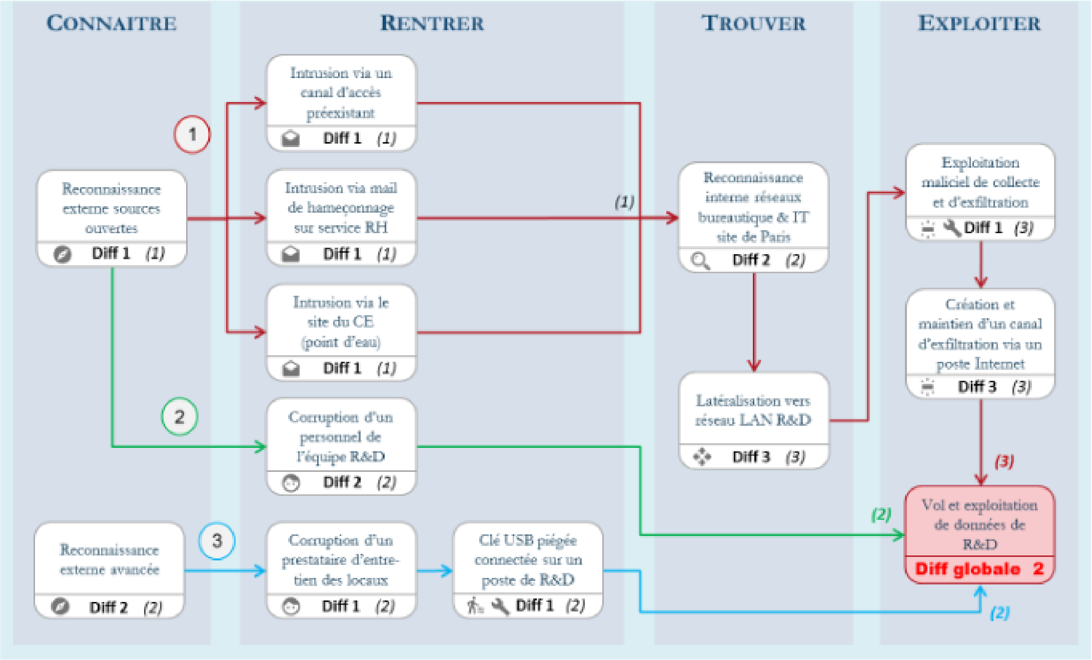


Échelle de difficulté technique d'une action élémentaire

Niveau de l'échelle	Description
4 – Très élevée	Difficulté très élevée : l'attaquant engagera des ressources très importantes pour mener à bien son action.
3 – Élevée	Difficulté élevée : l'attaquant engagera des ressources importantes pour mener à bien son action.
2 – Modérée	Difficulté modérée : l'attaquant engagera des ressources significatives pour mener à bien son action.
1 – Faible	Difficulté faible : les ressources engagées par l'attaquant seront faibles.
0 – Négligeable	Difficulté négligeable, voire nulle : les ressources engagées par l'attaquant seront négligeables ou déjà disponibles.

The advanced method allows an appreciation thinner likelihood: it takes in account the level of expertise and resources which the attacker will need to conduct his attack, also taking in to account the security of the target system. In fact, this method allows to consider the return on investment for the attacker and therefore to build a strategy of risk management driven by a logic of discouragement.

The rating criteria "technical difficulty and probability of success" are not rigorously independent. However, the "technical difficulty" is more particularly related to the level of protection of the target (its exposure and its vulnerabilities), while "probability of success is more influenced by its level of defence and Resilience (Supervisory, Incident Response and Continuity capabilities of activity).


CONNAITRE
RENTRER
TROUVER
EXPLOITER
1
2
3
Reconnaissance externe sources ouvertes
Diff 1 (1)
Reconnaissance externe avancée
Diff 2 (2)
Intrusion via un canal d'accès préexistant
Diff 1 (1)
Intrusion via mail de hameçonnage sur service RH
Diff 1 (1)
Intrusion via le site du CE (point d'eau)
Diff 1 (1)
Corruption d'un personnel de l'équipe R&D
Diff 2 (2)
Corruption d'un prestataire d'entre-tien des locaux
Diff 1 (2)
Clé USB piégée connectée sur un poste de R&D
Diff 1 (2)
(1)
Reconnaissance interne réseaux bureautique & IT site de Paris
Diff 2 (2)
Latéralisation vers réseau LAN R&D
Diff 3 (3)
Exploitation maliciel de collecte et d'exfiltration
Diff 1 (3)
Création et maintien d'un canal d'exfiltration via un poste Internet
Diff 3 (3)
(3)
(2)
Vol et exploitation de données de R&D
Diff globale 2
(2)

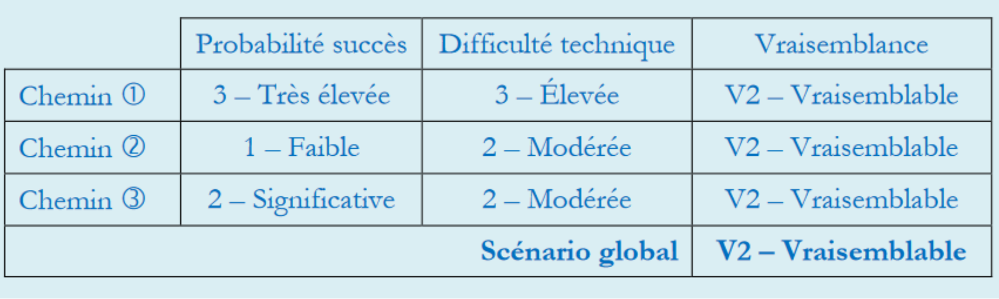
Let us plot another example which also illustrates the above scenario, but here the calculation of difficulty levels takes place for each node. After acquiring some knowledge about the external sources which are open (Difficulty Diff 1), the attacker can enter into the system in two main different ways. The first one indicated in red coloured (number 1, which has three elementary actions) and the second one indicated in green colour 2. There is a third way (blue coloured 3) which is based on the advanced external knowledge (Difficulty Diff 2). The difficulty level for each elementary action 'AE' is calculated according to the equation above.

For example, calculating the difficulty of first node under "Trouver",

$$\begin{aligned} \text{Indice\_Diff}\ (AE_{Diff\ 2}) &= \text{Max}\ \{\text{Indice\_Diff}(AE_{Diff\ 2),}\ \text{Min}(\text{Indices\_Diff}(AE_{Diff\ 1}\ ,\ AE_{Diff\ 1},\ AE_{Diff1}))\} \\ &= \text{Max}\ \{2,\ \text{Min}\ (1,1,1)\} \\ &= \text{Max}\ \{2,1\} \\ &= 2 \end{aligned}$$

Like this, we calculate for each nodes (AE). And obtain a final difficulty value for each path. The value for the first path being (3), the second path being (2) and the third path being (2).

The technical difficulty of the scenario is estimated globally as " 2 - Moderate", the modes least technically challenging being numbered ones and considering the probabilities of success previously evaluated, it is possible to establish the following synthesis:



	Probabilité succès	Difficulté technique	Vraisemblance
Chemin ①	3 – Très élevée	3 – Élevée	V2 – Vraisemblable
Chemin ②	1 – Faible	2 – Modérée	V2 – Vraisemblable
Chemin ③	2 – Significative	2 – Modérée	V2 – Vraisemblable
		Scénario global	**V2 – Vraisemblable**

Once we plot the "three values we obtain from the probability calculation using standard method" vs the "three values obtained from the technical difficulty calculation using Advanced method", we obtain the overall likelihood value (using Express method).

The three operating modes considered in the attack graph have the same level of likelihood. It leads to a likelihood "V2-Vraisemblable" for the scenario. By report to evaluation performed with the method standard (V3), the estimated likelihood is lesser: considering the criterion of technical difficulty brings a weighting on the estimate of the level of likelihood. Indeed, if the operating mode appears to have the most successful probability of success it also presents a technical difficulty relatively high.

About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **SGS**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), laboratories (**CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com