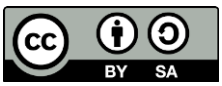
CLUBEBIOS

EBIOS RISK MANAGER

# How to manage baseline findings within EBIOS RISK MANAGER?

| | | |
|---|---|---|
| Date | : | 20/03/2026 |
| Status | : | Validated |
| Classification | : | Public |
| Number of pages | : | 9 |
| Project Manager | : | Ian GRISPAN |
| Validation | : | Practitioners' Committee |
| Approbation | : | Club EBIOS Board |
| License | : |  |



This document has been realized by le Club EBIOS

Club EBIOS, 11 rue de Lourmel, 75015 PARIS

Project Manager:

- Ian GRISPAN

Contributor(s) :

- Thomas FITOUSSI
- Damien AUVRAY
- Nicolas VAN CAUTER
- Mohammed HEBBAR

# Document History

| Date | Modification objective | Author(s) | Statut |
|---|---|---|---|
| 1.0 | Initial version | Practitioners' Committee | Validated |

# Table of contents

# 1. Purpose of the document

This document proposes a structured approach to transform baseline security non-compliances into useful inputs for risk analysis within EBIOS RM.
A non-compliance is not merely a "gap to be filled," but a triggering factor likely to influence attack paths (Workshop 3), operational scenarios (Workshop 4), and/or contribute to the risk treatment plan (Workshop 5).

# 2. Definitions

**RISK (EBIOS RM Guide v1.5)**: Possibility that a feared event occurs and that its effects impact the missions of the object of the study. In the cyber context in which EBIOS Risk Manager is situated, a risk is described in the form of a risk scenario.

**Risk scenario (INTENTIONAL) (EBIOS RM Guide v1.5)**: Complete scenario, going from the risk source to the objective targeted by it, describing an attack path and the associated operational scenario. NOTE: in the context of this guide, only intentional digital risk scenarios are considered. **For unintentional risks, see the method sheet from the college of practitioners: How to treat unintentional risks.**

**Security baseline (EBIOS RM Guide v1.5):** It is the expression of measures:

- allowing to treat non-deliberate or non-targeted risks (often relying on standard frameworks);
- which do not require to be justified by a scenario-based approach (workshops 3 and 4). In particular, measures from frameworks or legislation whose application is mandatory and without interpretation.

Measures of the security baseline are an integral part of the risk treatment plan, in the same way as the other measures from workshops 3, 4 and 5.

**Non-compliance:** proven deviation from a baseline requirement. It may concern technical components, processes, data, or external stakeholders (providers, SaaS/IaaS/PaaS, partners, subsidiaries) through contractual commitments. The analysis of these gaps may come from audit results or previous gap analyses.

**Exploitability:** capacity, for a risk source, to convert the deviation into an opportunity in an attack path (workshop 3) then into a concrete operational mode (workshop 4).

**Elementary Action:** unit action executed by a risk source on a supporting asset in the context of an operational scenario.

**Security measure (EBIOS RM Guide v1.5):** Means of treating a risk taking the form of solutions or requirements that can be included in a contract.

**Vulnerability:** Fault, through malice or clumsiness, in the specifications, design, implementation, installation or configuration of a system, or in the way it is used. A vulnerability can be used by an exploit code and lead to an intrusion into the system.

# 3. Integration into EBIOS RM: articulation of workshops

**Workshop 1 — Framing & baseline:**
Identify and qualify deviations from baseline security (hygiene, regulatory, normative, contractual).
For deviations affecting supporting assets, they may be translated into vulnerabilities and stored in a vulnerability catalog.

**Workshop 3 — Strategic scenarios:**
Relevant and exploitable non-compliances are analyzed to determine whether they can serve as attack vectors, especially via stakeholders.

**Workshop 4 — Operational scenarios:**
Non-compliances (translated into vulnerabilities) can feed operational modes in the form of elementary actions.

**Workshop 5 — Treatment:**
All measures are consolidated into the risk treatment plan:

- Measures from Workshop 1 addressing baseline deviations linked to scenarios;
- Contextual measures from Workshop 2;
- Stakeholder-related measures from Workshop 3;
- Action-based measures from Workshop 4.

# 4. Four-step operational approach

**1) Identify the non-compliances of the security baseline during workshop 1.** Make a list of deviations non-compliant with the security baseline. Also add any ad hoc measures identified during workshop 2, for example IoC specific to risk sources or targeted objectives.

**2) During workshop 3.** Analyze the deviations of this list during workshop 3 to determine whether one of them can be exploited in the context of attack paths. The objective is to identify and qualify any new plausible path and its effect due to this non-compliance / vulnerability.

To do this it is important to link the justifications of danger levels or selected attack paths to these non-compliances.

**3) During workshop 4.** Analyze the deviations of this list during workshop 4 to determine whether one of them makes it possible to identify additional concrete operational modes: sequences of actions allowing the risk source to reach its targeted objective. A preliminary step that can facilitate this is to transpose the non-compliances applicable to supporting assets into vulnerabilities contextualized to these supporting assets, in a "vulnerability catalog" of the system.

**4) During workshop 5:** Consolidate the treatment of non-compliances. Link each measure of the Risk Treatment Plan to a risk scenario. The Risk Treatment Plan can contain measures that cover one or more risks. During the consolidation of non-compliance in the RTP, it may be useful to be able to identify the origin of security measures: non-compliances of the security baseline, vulnerabilities from audit results, "additional" measures on elementary actions (see workshop 4).

## 5. Risks of drift

The risk of drift observed in the consideration of the results of the study of the security baseline is the creation of a compliance tunnel effect.

**Compliance tunnel.** The temptation to mechanically and directly transform compliance gaps into risks can obscure the reflection linked to a scenario-based approach.

- **We move away from the definition of risk according to EBIOS RM.** In EBIOS RM, a risk is formed by a complete scenario: it links a risk source to a targeted objective, by explaining an attack path (workshop 3) and an operational scenario (workshop 4). A non-compliance described in isolation (e.g. "no strong authentication") is not a risk: it says nothing about who could attack us, what their objective would be, how they achieve their objective and how this would impact our business values, all these elements are treated through workshops 2 and 3.

- **Limitation of feasibility (workshop 4).** Without an operational scenario, it is impossible to verify upstream exploitability (can the attacker put themselves in a position to exploit the gap?) and downstream (can they, after exploitation, reach their objective — exfiltrate, alter, interrupt?). Workshop 4 is precisely used to test these hypotheses in order to determine if these scenarios are 'feasible'.

*In order to avoid this **compliance tunnel effect**, it is important **not to record baseline non-compliances as "risks" as such in the risk** summary of workshop 5 because this circumvents the principle of a scenario-based approach.*

# 6. Points of attention

Focus on deviations from the security baseline:

**NOTE:** *In substance it is always possible to associate / illustrate a non-compliance with the baseline by/in a risk scenario. But it is only to be taken into consideration if this scenario is relevant in the study and the context of the studied system.*

It must be kept in mind that intrinsically all the requirements it contains come from a risk scenario that has already been formalized somewhere, in the past… and often multiple times!

Hence the interest of the security baseline in saying to oneself that if we systematically find a set of scenarios whose way of covering them is always done with the same security measures (typically the case of basic scenarios), it will always be less costly to directly announce the systematic implementation of these measures (i.e. the "security baseline") and then verify that it is sufficiently (and correctly) implemented, rather than reinventing the wheel systematically (cf. the change of paradigm between EBIOS RM and previous versions of EBIOS).

If we want the detail of these basic scenarios, the work of the German BSI and more precisely their IT-Grundschutz-Kompendium, propose a rather exhaustive (and regularly updated) cross-reference between each security measure and each elementary threat... (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

# 7. Conclusion

By default, all measures deemed relevant resulting from the different workshops associated with a risk scenario must be recorded in the Risk Treatment Plan. If no risk scenario is retained concerning a security measure resulting from a deviation from the security baseline (demonstrated non-exploitability, robust compensating controls), this should not be recorded in the RTP.

**NOTE:** *The risk treatment plan is the document that groups together the measures allowing to treat risks, its objective is to be able to prioritize these measures with regard to the level of the most important risks that they cover.*

Indeed, putting measures not linked to a risk in the RTP makes it possible to have all the measures in a single document, however this exposes you to the following limits:

- Measures not being linked to a risk, it will be difficult to reach the objective and usefulness of the RTP, namely, to prioritize the application of measures according to the level of risk that they cover.
- It will also be more difficult to justify the application of these measures to an authority apart from the application of the concept of defense in depth.