CLUBEBIOS

EBIOS RISK MANAGER – Method sheet

How to deal with unintentional aspects with EBIOS RISK MANAGER?

Date	:	08/05/2026
Status	:	Valid
Classification	:	PUBLIC – UNPROTECTED
Page names	:	17
Project Manager	:	Ian GRISPAN
Validation	:	Working group
Approbation	:	Board of Directors
Licence	:	

This document was produced by the EBIOS Club and translated by Gemini

Club EBIOS, 11 rue de Lourmel, 75015 PARIS

Project manager(s):

- Ian GRISPAN - Airbus PROTECT

Contributor(s):

- Damien AUVRAY
- Jean OLIVE – CGI Business Consulting
- Stéphane PAUL
- Zian DELAHAYE

Change history

Date	Purpose of the modification	Author(s)	Status
20/04/2026	Consolidated initial version — expanded scope (purely unintentional risks and unintentional factors in intentional scenarios)	College of Practitioners	Working document
06/05/2026	Consolidation following arbitration by the College: scope maintained at 2 forms (Option A); integration of feedback from D. Auvray (terminology "factor" / "element"), J. Olive (clarification of §1.4 targeted SI, ecosystem variant §2.3), Z. Delahaye (validation); correction of typos; reformulation of §3.5	I. GRISPAN	Working document
08/05/2026	Version Finale	I.GRISPAN	Valid

CC BY

Summary

1 INTRODUCTION 6

2 CONCEPTS AND SCOPE 7

2.1 DEFINITION OF UNINTENTIONAL RISK 7

2.2 TYPOLOGY OF UNINTENTIONAL RISK SOURCES 7

2.3 TWO TREATMENT APPROACHES 8

2.4 BORDERLINE CASE: ACCIDENTAL EVENT DELIBERATELY CAUSED 8

3 APPROACH A: ADDRESSING A PURELY UNINTENTIONAL RISK 9

3.1 PRINCIPLE 9

3.2 STEP 1: GATHER THE INPUT ELEMENTS 9

3.3 STEP 2: IDENTIFY A TRIGGERING EVENT 9

3.4 STEP 3: LINK THE TRIGGERING EVENT TO A FEARED EVENT 10

3.5 STEP 4: DESCRIBE THE PROCEDURE 10

3.6 STEP 5: ESTIMATE THE LIKELIHOOD 10

3.7 STEP 6: INTEGRATE INTO WORKSHOP 5 11

4 APPROACH B: INTEGRATING AN UNINTENTIONAL FACTOR INTO AN INTENTIONAL SCENARIO 12

4.1 PRINCIPLE 12

4.2 CONSIDERATION IN WORKSHOP 2 12

4.3 CONSIDERATION IN WORKSHOP 3 12

4.4 CONSIDERATION IN WORKSHOP 4 12

4.5 WORKSHOP PROCESSING 5 13

5 CHOOSE THE APPROACH ACCORDING TO THE CONTEXT 14

6 TABLE OF TYPICAL TRIGGERING EVENTS 15

6.1 TRIGGERING EVENTS OF ACCIDENTAL ORIGIN 15

6.2 ENVIRONMENTAL TRIGGERING EVENTS 15

7 CONCLUSION 16

8 ANNEXES 17

8.1 ACRONYMS 17

CC BY

8.2 GLOSSARY 17

8.3 BIBLIOGRAPHY 17

1 Introduction

The EBIOS Risk Manager method addresses cybersecurity risks using two complementary approaches:

1. The compliance approach defines a security base sized for the most common risks, including the most frequent unintentional risks.
2. The scenario-based approach identifies advanced risks of intentional origin, particularly targeted or sophisticated attacks.

The EBIOS RM guide repeatedly mentions the category of unintentional or untargeted risks. When such risks are identified during the baseline or feared event analysis, the guide stipulates that they be integrated into the risk matrix so that appropriate measures can be included in the treatment plan. In practice, these risks take two distinct forms, each requiring a different approach.

This sheet covers both forms.



On the one hand, unintentional risks in the strict sense, in which a triggering event of accidental or environmental origin directly causes a feared event, without voluntary intervention by an attacker.

On the other hand, there are unintentional factors that facilitate a scenario of intentional attack.by opening a breach, degrading a security measure, or providing a means of access to a malicious risk source.

These two situations share the same root cause, the absence of intent to harm on the part of the human actor or the non-human origin of the generating event, but they are translated differently in the method.

The guide offers, for each situation, an operational approach as close as possible to the standard practice of EBIOS RM. It is intended for practitioners who already have a mastery of the method and who wish to enrich their studies with an explicit consideration of unintentional factors.

CC BY

2 Concepts and scope

2.1 Definition of unintentional risk

The EBIOS Risk Manager method typically describes a cybersecurity risk as a scenario progressing from a risk source to its intended objective. This formulation, geared towards deliberate risks, assumes an intent to harm.

For unintentional risks, this document uses the following definition:

"An unintentional risk is the possibility that a feared event may occur as a result of a triggering event, without any intention to harm."

Two complementary concepts are used throughout the document:

- **Triggering event:**accidental human, technical or environmental cause that led to a feared event or an action subsequently exploited by an attacker.
- **Associated vulnerability:**a defect or weakness in the system that makes it possible for the triggering event to lead to the feared event, or that increases the likelihood of an elementary action in an intentional scenario.

2.2 Typology of unintentional risk sources

Unintentional sources fall into two categories:

Accidental (human) sources. Human stakeholders (employees, service providers, visitors) may, through error, omission, inattention, or lack of competence, cause an incident without intent to harm. Examples: incorrect handling, sending a file to the wrong recipient, accidental deletion, forgetting a step in a procedure, unintentional disclosure of login credentials.

Environmental sources. Events or phenomena external to human activity within the perimeter, of a physical or natural nature, as well as hardware failures and software bugs. Examples: health crisis, fire, flood, power outage, hardware failure, software bug, weather event.

By convention, hardware failures and software bugs are linked to the environmental category: although internal to the system, they do not result from a voluntary human action and share with environmental phenomena the absence of an intentional actor.

CC BY

2.3 Two treatment approaches

The document distinguishes two treatment approaches, depending on the role of the unintentional factor in the scenario.

Approach A: Purely unintentional risk. An unintentional triggering event directly causes a feared event, without the intervention of a malicious risk source. Detailed treatment in Chapter 3 (six-step empirical approach).

Approach B: An unintentional factor in an intentional scenario. An unintentional event (human error, negligence, failure) creates an element that a malicious risk source exploits in its attack path. Detailed treatment in Chapter 4 (integrated into workshops 2 to 4).

These two approaches are not mutually exclusive: an EBIOS RM study can combine them depending on its context. Chapter 5 provides guidelines for choosing the appropriate approach based on the study's objective.

2.4 Borderline case: accidental event deliberately caused



And**accidental or environmental event**may be deliberately caused by an intentional risk source targeting the studied IS: fire started maliciously to force an evacuation, power outage orchestrated to interrupt a service.

In these situations, the risk is intentional and must be dealt with using a classic scenario, not this guide.

The accidental form of the generating event does not presume the unintentional nature of the risk; it is the absence of intention that characterizes the unintentional.

CC BY

3 Approach A: Addressing a purely unintentional risk

3.1 Principle

The approach is deliberately empirical.

It aims to integrate unintentional risks into the risk matrix without resorting to the full formalism of workshops 2, 3 and 4 of the EBIOS RM method.

Unintentional risk is constructed from a deviation from the security baseline or an identified feared event, characterized by a simple triggering event.

The approach unfolds in six short steps that can be carried out quickly, including as a complement to a workshop already held.

3.2 Step 1: Gather the input elements

The input elements are the list of feared events established in workshop 1 with their associated severity, the list of deviations from the security baseline identified, and, where applicable, the environmental risk analyses already available (flood study, fire analysis).

A deviation from the baseline or a feared event that gives rise to a potential unintentional risk becomes a candidate for the next step in the process.

3.3 Step 2: Identify a triggering event

For each candidate element selected in the previous step (deviation from the baseline, feared event or environmental risk analysis), a formulation of the most plausible unintentional triggering event must be expressed, specifying the source of unintentional risk to which it relates (accidental or environmental, see typology §2.2) as well as the associated vulnerability.

Example : Accidental destruction of production data by a system administrator → vulnerability: lack of validation control before execution of critical commands (e.g. rm -rf launched on the wrong environment).
The administrator has no intention of causing harm. The harmful action is purely accidental. There is no malicious third-party actor involved.

The triggering events can occur directly on the information system under study or within its ecosystem (hosting provider, critical supplier, third-party service) and propagate to it. In all cases, the link to the feared event remains direct and must be addressed here and outside of workshop 3.

CC BY

3.4 Step 3: Link the triggering event to a feared event

For each identified triggering event, the question is asked: can this event cause a feared event from workshop 1? If yes, the link is established; otherwise, the risk is not relevant for the study.

Example Accidental destruction of production data by a system administrator → Irretrievable loss of critical business data (feared event).

The severity of the unintentional risk is that of the feared event, as assessed in workshop 1. It does not need to be reassessed.

3.5 Step 4: Describe the procedure

Without reconstructing a complete operational scenario, it is recommended to describe in a few words how the triggering event could lead to the feared event. This concise operating procedure makes the risk understandable and controllable in workshop 5.

Example : Accidental destruction of production data by an administrator → lack of validation checks before execution of critical commands → undetected and unblocked deletion → overwriting of production data with no possibility of immediate rollback → unavailability of the affected business service

3.6 Step 5: Estimate the likelihood

The likelihood is estimated in an "express" mode, without reconstructing a sequence of elementary actions.

It reflects the probability that the sequence described in step 4 will occur over the period considered, taking into account the measures of the actual foundation in place and any available statistical indicators (incident history, environmental studies).

If you do not have your own scale, you can use the scale below:

Level	Label	Description indicative
1	Rare	May occur in exceptional circumstances, less than once every 10 years.
2	Unlikely	It can occur but is not expected (typical frequency: 5 to 10 years).
3	Probable	May occur occasionally (typical frequency: 1 to 5 years).
4	Quasi certain	Occurs frequently or continuously.

CC BY

For accidental risks, the assessment takes into account the observed recurrence (previous incidents), the familiarity of the actors with the tasks concerned, the overload of the actors at the origin of the generating event, the level of training, the availability of procedures, and the detection and correction mechanisms (four-eye control, supervision).

For environmental risks, the assessment is based on existing analyses and on prevention and detection measures already deployed.

3.7 Step 6: Integrate into workshop 5

Once the severity (inherited from workshop 1) and likelihood (estimated in step 5) have been established, the unintentional risk is inserted into the risk matrix. It is then addressed in workshop 5 according to the same logic as intentional risks: acceptance, reduction, avoidance, transfer.

Treatment measures are defined on a case-by-case basis, but may be common to those for intentional risks.

For accidental sources, they may aim at strengthening the selection and qualification of human resources, strengthening teams, training, providing procedures and guides, and deploying manual or automated controls.

For environmental sources, they can target avoidance (relocation), crisis management mechanisms, business continuity and recovery plans.

CC BY

4 Approach B: Integrating an unintentional factor into an intentional scenario

4.1 Principle

In this approach, the unintentional factor is not the origin of the risk but an element that increases its likelihood or opens up a previously blocked avenue of attack.

The risk scenario remains intentional: it has a malicious risk source, a targeted objective, and an attack path. The unintentional factor is integrated into it in the same way as a vulnerability exploited by the attacker.



The approach remains faithful to workshops 2 to 4 of the EBIOS RM method. It does not introduce any new structuring concept: unintentional factors are treated as elementary actions of the operational scenario, with their consequences on plausibility.

4.2 Consideration in workshop 2

Workshop 2 identifies relevant risk source/target objective pairs. For a scenario likely to be facilitated by an unintentional factor, no adaptation is necessary at this stage: the source remains malicious, the objective remains a desired benefit.

The question of the unintentional factor will be addressed later in the analysis, when the attack path is specified.

4.3 Consideration in workshop 3

The strategic scenarios developed in workshop 3 may involve stakeholders whose unintentional actions could be exploited by the source of risk. This does not require any methodological changes: the stakeholder is identified according to standard practice.

4.4 Consideration in workshop 4

It is in workshop 4 that the unintentional factor is explicitly addressed in the approach. The operational scenario describes a series of elementary actions carried out by the attacker. When one of these actions relies on an unintentional factor, this factor is explicitly stated in the operational procedure and taken into account in the likelihood assessment.

CC BY

Two complementary practices are recommended:

1. **Document the unintentional factor in the operational scenario.**Rather than masking it in the formulation of an elementary action, name it explicitly.

   Example :Instead of writing "The attacker obtains valid credentials", write "The attacker obtains valid credentials left on a sticky note by a collaborator".

The traceability of the unintentional factor is thus preserved for workshop 5.

2. **To modulate the likelihood of the elementary action in question.**The likelihood of the elementary action benefiting from the unintentional factor is assessed by taking into account the expected frequency of this factor (history of incidents, level of cyber maturity of the actors involved, weakness of existing compensatory measures).

   Example : A scenario for exfiltrating R&D data is facilitated by the fact that the system does not guarantee that an employee will not share their remote access credentials via personal messaging.

   The operational scenario then includes an elementary action "Acquisition of valid credentials via an insecure channel" whose likelihood is assessed by taking into account the history of incidents and the presence (or absence) of multi-factor authentication which would make credentials insufficient on their own.

4.5 Workshop processing 5

The processing of the intentional scenario takes place in workshop 5 according to standard practice.

However, the presence of an unintentional factor as a facilitating element opens up a range of specific complementary measures:

- targeted awareness-raising of relevant stakeholders;
- technical controls that reduce the impact of unintentional behavior (multi-factor authentication, sharing monitoring, data leak detection);
- improvement of ambiguous or restrictive procedures that encourage unintentional workarounds.

CC BY

5 Choose the approach according to the context

The choice of one, the other, or both approaches depends on the nature of the object of the study and the risks that characterize it.

The following three cases cover typical situations encountered in EBIOS RM studies.

Case 1: Object primarily exposed to unintentional risks. Typically, this is a data center, a proprietary hosted infrastructure, and an environment with a strong focus on operational safety. Approach A is central. Approach B can remain implicit if no significant intentional attack scenario is considered in the study.

Case 2: Object primarily exposed to intentional risks. Typically, this involves a web service exposed on the internet, a SaaS platform, or a consumer application. Approach B is central. Approach A can be addressed briefly to cover the few purely unintentional risks identified (hosting provider failure, update bug).

Case 3: Object exposed to both types of risks. Typically, this involves a self-hosted enterprise information system or a hybrid ecosystem (hosted infrastructure and services). Both approaches are used together. This is the most common scenario.

This breakdown is a guideline, not a prescription. In all cases, the final decision rests with the study leader, based on the objectives assigned to the risk analysis and the expected deliverables.

CC BY

6 Table of typical triggering events

The table below provides a guide for identifying a triggering event (Approach A) or an unintentional factor (Approach B). It is neither exhaustive nor prescriptive: the triggering events selected depend on the context of the subject of the study.

6.1 Triggering events of accidental origin

Typical triggering event	Example
Handling error	Accidental deletion of a production database.
Incorrect submission	Sending a sensitive document to the wrong recipient.
Failure to comply with a procedure	Maintenance performed without following the prior backup process.
Incorrect configuration	Unintentional opening of a service to public access.
Oversight	No account deactivation upon departure.
Loss or misplacement	Loss of mobile equipment containing sensitive data.
Unintentional disclosure	Sharing of identifiers via messaging, publication of data on an uncontrolled public service.
Convenience bypass	Temporary deactivation of a security measure to perform a task more quickly, without reactivation.

6.2 Environmental triggering events

Typical triggering event	Description
External fire	Fire originating outside the site, which could spread or cause an evacuation.
Internal fire	Fire caused by electrical failure or faulty equipment.
Flood	Rising water levels or burst pipes.
Climate phenomenon	Storm, heavy rain, heat wave.
Seismic phenomenon	Earthquake affecting buildings and infrastructure.

CC BY

Power outage	Power outage.
Cooling system failure	Critical equipment overheating.
Network loss	Telecommunications services unavailable.
Health crisis	Staff unavailability and organizational constraints.
Hardware failure	Critical equipment failure.
Software bug	Code defect causing a malfunction.

7 Conclusion

The treatment of unintentional events in an EBIOS RM study is based on two complementary approaches.

Approach A, purely non-intentional, incorporates risks whose origin is accidental or environmental; it mobilizes an empirical approach in six steps, anchored on the severity of workshop 1 and the treatment in workshop 5.

Approach B, a mixed approach, integrates unintentional factors into intentional scenarios; it is based on workshops 2 to 4 without structural modification of the method, by making the unintentional factor explicit in the operational scenario and integrating it into the likelihood assessment.

The safety framework, even when perfectly applied, does not cover all plausible accidental situations, nor the operational gaps that actually exist on the ground (inapplicable requirements, derogations, blind spots in the reference framework).

Unintentional risks often have significant direct consequences and can, in some cases, exacerbate intentional scenarios with which they combine. Explicitly addressing them in the EBIOS RM study strengthens the overall quality of the analysis and the relevance of the treatment plan.

The approach proposed in this document is designed to be compatible with existing practices and adaptable to the context of the study, without significantly increasing the complexity of the process. It may be further developed by subsequent work from the College of Practitioners, particularly on multifactorial risk analysis and alternative classifications of risk sources.

CC BY

8 Annexes

8.1 Acronyms

ANSSI	National Cybersecurity Agency
EBIOS RM	Statement of Needs and Identification of Security Objectives — Risk Manager
IS	A dreaded event
SR	Source of risk
OV	Target
AND	Information system
R&D	Research and Development
SaaS	Software as a Service

8.2 Glossary

Unintentional risk	The possibility that a feared event could occur as a result of a triggering event, without intent to harm.
Triggering event	Accidental human, technical or environmental cause that led to a feared event or an action subsequently exploited by an attacker.
Source of accidental risk	A human stakeholder who, through error, omission, inattention or lack of competence, may cause a triggering event without intent to harm.
Source of environmental risk	An event or phenomenon external to human activity within the perimeter (physical, natural) or a hardware/software failure likely to cause a feared event.
Unintentional factor	An unintentional event that, in an intentional attack scenario, creates or exacerbates an element exploited by a malicious risk source.
Approach A	Handling purely unintentional risks, without the intervention of a malicious risk source.
Approach B	Taking into account unintentional factors as facilitating elements within intentional scenarios.
(Unintentional) modus operandi	A concise description of the sequence of events by which a triggering event leads to a feared event, without reconstructing a complete operational scenario.

CC BY

8.3 Bibliography

The following references appear in brackets in this document.

• [ANSSI-EBIOS-RM-V1.5] ANSSI, The EBIOS Risk Manager method — The guide, version 1.5, 2024.
• [ANSSI-EBIOS-RM-FICHES] ANSSI, EBIOS Risk Manager — Method sheets, 2018-2024.