Item	Content
Document No.	CRA-RA-001
Version	V1.0
Date	2 September 2026
Prepared by	Jin Cancan
Reviewed by	Zhou Yang
Approved by	Zhou Yang
Product	Nand Flash Tracer (NFT), software only, assessment baseline version Ver 2.26.8
Language	English version - Official Version for EU Market Surveillance Authorities

Cybersecurity Risk Assessment (Regulation (EU) 2024/2847, Article 13)

Note: The Chinese version of this document (CRA-RA-001 V1.0, Internal Working Version) is the internal working version. The two versions are identical in section structure, table numbering, risk scores and compliance conclusions. The CRA does not prescribe a language for the technical documentation (this product follows Module A, with no notified body involved); the EU declaration of conformity and the user information and instructions are to be made available in the language required by the Member State in which the product is made available.

Note: This document is the cybersecurity risk assessment referred to by the Technical Documentation CRA-TD-001 (Annex VII, point 3). The compliance mapping table in Annex B of CRA-TD-001 is consistent with this document. In the event of any inconsistency, ***this document prevails*** *and CRA-TD-001 is to be revised accordingly.*

1. Purpose and legal basis

1.1 Purpose

This document records the cybersecurity risk assessment carried out by Dalian ByteSmart Technology Co., Ltd. (the "manufacturer") in respect of its product Nand Flash Tracer ("NFT" or the "product"). It serves to:

1. Identify the cybersecurity risks to which the product is exposed across the lifecycle phases of design, development, production, delivery, deployment and use, maintenance and update, and decommissioning;
2. Determine whether and how each of the essential requirements in Annex I, Part I, point (2), sub-points (a) to (m) of Regulation (EU) 2024/2847 (the "Cyber Resilience Act" or "CRA") applies to the product, and give explicit reasons for any requirement that does not apply;
3. Explain how Annex I, Part I, point (1) and the vulnerability handling requirements in Part II apply;
4. Provide the risk basis for the Technical Documentation CRA-TD-001 and the Test Report CRA-TR-001, so that design and test coverage can be traced back to risk.

1.2 Legal basis

Legal basis	Substance	Implementation in this document
Article 13(2)	The manufacturer shall carry out a cybersecurity risk assessment and take its results into account during the planning, design, development, production, delivery and maintenance phases, with a view to minimising cybersecurity risks, preventing incidents and minimising their impact, including in relation to the health and safety of users	Section 5 organises threat scenarios by lifecycle phase; Section 8 sets out treatment; Section 9 explains how the results were taken into account
Article 13(3)	The risk assessment shall be documented and kept up to date during the support period; it shall include at least a risk analysis based on the intended purpose and reasonably foreseeable use and conditions of use (such as the operating environment and the assets to be protected), and shall take into account the expected lifetime of the product; it shall **indicate whether and how each of the security requirements in Annex I, Part I, point (2) applies**, and how Annex I, Part I, point (1) and the Part II vulnerability handling requirements apply	Sections 2 and 3 (scope and assets); Section 6 (sub-point-by-sub-point determination for (a) to (m)); Section 7 (Part II); Section 10 (update and maintenance); support period in CRA-TD-001, Section 6
Article 13(4)	The risk assessment shall be included in the technical documentation; **where certain essential requirements do not apply, the manufacturer shall include clear reasons in the technical documentation**	Section 6 gives explicit reasons for every "not applicable" or "partially applicable" determination
Article 13(7)	The manufacturer shall systematically record relevant cybersecurity matters in a manner proportionate to the nature and risks, including vulnerabilities of which it is aware and information provided by third parties, and shall update the risk assessment as appropriate	Section 10
Annex VII, point 3	The technical documentation	This document in its entirety

	shall contain the cybersecurity risk assessment carried out pursuant to Article 13 at the design and development, production, delivery and maintenance stages, including whether the essential requirements in Annex I, Part I apply	

Reference: Regulation (EU) 2024/2847, Article 13(2), (3), (4) and (7); Annex VII, point 3.

1.3 Relationship with other documents

Document No.	Title	Relationship to this document
CRA-CLASS-001	Product Scope and Classification Record	Provides the classification (default/standard category, Module A) on which this assessment relies
CRA-TD-001	Technical Documentation	Refers to this document as the Annex VII point 3 risk assessment; its Annex B is consistent with this document
CRA-TR-001	Test Report	Verifies the verifiable items arising from the treatment measures in Sections 5 and 8
CRA-SBOM-001	Software Bill of Materials	Supports the supply-chain threats in Section 5 and Part II point (1) in Section 7
CRA-VHP-001	Vulnerability Handling Procedure	Supports Section 7 and the maintenance and update risks in Section 8
CRA-CVD-001	Coordinated Vulnerability Disclosure Policy	Supports T-14 and T-21 in Section 5
CRA-IRP-001	Incident and Vulnerability Reporting Procedure	Supports T-21 and the exercise in CRA-TR-001, Section 7
CRA-SUP-001	Security Update Distribution Procedure	Supports sub-point (c) in Section 6 and Part II points (2), (7) and (8) in Section 7
CRA-DoC-001	EU Declaration of Conformity	Its statement of conformity relies, among other things, on the conclusions of this assessment

2. Scope and object of the assessment

2.1 Object of the assessment

Item	Content
Product name	Nand Flash Tracer (NFT)
Product type	Software only; locally installed data recovery and reconstruction tool

Assessment baseline version	**Ver 3.26.8.26** (internal build identifier:)
CRA classification	Default / standard category
Conformity assessment procedure	Module A, Annex VIII, Part I (internal production control, self-assessment, no notified body involved)
Support period	10 February 2024 to 10 February 2029 (5 years)
Operating environment	Windows 7 / 10 / 11; local stand-alone installation; no cloud service; no remote data processing
Network use	Licence activation (device binding verification) and update checking only

Note on versions: CRA-CLASS-001 V2.1 records version Ver 2.26.0617, whereas the assessment baseline version of this document is Ver 2.26.8. Both belong to the 2.26 series, core functionality is unchanged, and the classification (default category, Module A) continues to apply.

2.2 In-scope boundary

This assessment covers:

5. The NFT installer, the main executable and its bundled runtime dependencies, the chip ID and configuration database files, and the default configuration templates;
6. The dump image import and parsing path, including the modules for virtual page reconstruction, ECC processing, bad block handling, XOR detection, Read-Retry, sector trimming and custom formula transformation;
7. The read and write paths for project files (job files and layout files);
8. The licence activation and device binding verification module and its sole outbound network interaction;
9. The update check, update download and update package verification mechanisms;
10. The logging, temporary file and uninstallation behaviour of the product;
11. The security properties of the manufacturer's official download channel (the download page on the official website) to the extent that it serves as a distribution channel for the product;
12. The cybersecurity-related content of the user information and instructions.

2.3 Out-of-scope boundary

The following are expressly **excluded**, and the manufacturer makes no statement of conformity in respect of them (reference: Regulation (EU) 2024/2847, Article 13(1), the obligations of the manufacturer concern the product it places on the market; Annex VII, point 1, the technical documentation describes the product itself):

13. **Chip reader hardware supplied by the user** (third-party flash programmers/readers) together with their drivers, firmware and bundled software. The manufacturer defines only the importable file formats and is not responsible for the cybersecurity properties of that hardware;

14. **Storage media supplied by the user** (USB drives, SD cards, TF cards, eMMC, consumer SSDs, IoT storage chips) and the **content** of dump images and project files generated by the user or by third parties. The product treats these files as untrusted input and validates them, but is not responsible for the lawfulness of their origin or for the nature of the data they contain;
15. **Content published on the manufacturer's website and forum**, including third-party and user-generated content. The website and forum are considered in this assessment only as they relate to "download distribution security" and to "social engineering impersonating the manufacturer" (see T-12, T-13 and T-14), not as to the compliance of their content;
16. **The host environment on which the user runs the product**: the Windows operating system, file system and disk encryption mechanisms, account and permission model, anti-malware software and network perimeter protection, as well as the user organisation's own processes and governance;
17. **Processing operations carried out by the user on recovered data.** Those operations are the responsibility of the user acting as data controller (see T-18);
18. **Circumvention of the licence and unauthorised redistribution.** This does not constitute a cybersecurity risk to the user's data or environment and is treated as a commercial risk to the manufacturer. It is recorded separately as T-25 and labelled honestly as such (see the note below the table in Section 5).

3. Register of assets to be protected

Reference: Regulation (EU) 2024/2847, Article 13(3) (the risk analysis is to take into account the assets to be protected).

Cybersecurity properties are abbreviated as follows: **C** confidentiality, **I** integrity, **A** availability.

No.	Asset	Cybersecurity property at stake	Owner / responsible role	Criticality
A-01	Software binaries and build artefacts (main executable, dynamic libraries, installer)	I, A	Head of R&D (Zhou Yang)	High
A-02	Licence activation and device binding mechanism (licence verification logic and local binding records)	I, A	Head of R&D (Zhou Yang)	Medium
A-03	Update distribution channel (official	I, A	Head of R&D (Zhou Yang);	High

	download page, update check endpoint, distribution server)			
A-04	Chip ID and configuration database files, default configuration templates	I	Head of R&D (Zhou Yang)	Medium
A-05	Job and layout project files (project data read and written by the product)	I, C, A	The user (self-managed); the product is responsible for format robustness	Medium
A-06	User dump images and recovered data	C, I, A	**The user**; the product neither retains nor uploads nor encrypts them and encounters them only during processing	High
A-07	Source code repository and build environment (build machine and toolchain)	C, I	Head of R&D (Zhou Yang)	High
A-08	Code signing key and activation server-side keys	C, I	Jin Cancan	High
A-09	Official website and forum	I, A	Zhou Yang	Medium
A-10	Host execution environment (memory, CPU, file system and network stack of the user's machine)	I, A	The user; the product is under a duty not to impair it (Annex I, Part I, point (2)(i))	High
A-11	Product logs and temporary files	C, I	Head of R&D (Zhou Yang)	Low
A-12	Manufacturer reputation and compliance standing	C, I, A	Compliance and documentation lead (Jin Cancan)	Medium

Note: A-06 (user dump images and recovered data) is owned and controlled by the user. By design the product neither retains, uploads nor encrypts that data. This assessment therefore addresses that asset from the standpoint that "the product must not, through its own defects, cause that data to be destroyed, disclosed or rendered unavailable", and that "the product must not come into contact with that data to an extent exceeding what is necessary".

4. Methodology

4.1 Statement on proportionality

A semi-quantitative risk matrix is used. The choice of method is proportionate both to the size of the manufacturer (a micro/small enterprise) and to the risk profile of the product:

19. The product is **software only, installed locally on a stand-alone machine, with no cloud component and no inbound listening ports**; its effective attack surface is concentrated in the local file import and parsing path (see CRA-TD-001, Section 3.3);
20. The product does **not process, store or transmit** data beyond what is necessary for its intended purpose, and has no remote management, remote execution or self-propagation capability;
21. A combination of structured threat modelling, semi-quantitative scoring and a requirement-by-requirement determination is therefore sufficient to meet the risk-based requirement of Article 13(2). **This assessment neither promises nor relies upon penetration testing by external firms or upon any third-party certification.** Verification is limited to static analysis, vulnerability scanning of dependencies, malformed input and fuzz testing, and process exercises that the manufacturer can carry out itself, all of which are recorded in CRA-TR-001.

Reference: Regulation (EU) 2024/2847, Article 13(2) (risk-based); Annex I, Part I, point (1) (appropriate level of cybersecurity based on the risks).

4.2 Likelihood scale

Level	Name	Definition
1	Rare	Very low likelihood of occurrence within the support period; would require a capable attacker, internal access rights or physical access
2	Unlikely	A known attack path exists but requires specific conditions to coincide, or imposes significant cost on the attacker
3	Possible	Publicly available attack methods or generic tooling exist, or the scenario may be triggered incidentally under normal conditions of use
4	Likely	Low attack cost, automatable, or virtually certain to occur in the absence of effective controls

4.3 Impact scale

Level	Name	Definition

1	Negligible	Almost no effect on user data, product functionality or the user's environment; or an effect confined to the manufacturer's own commercial interests, not touching the security of the user's data or environment
2	Limited	Transient degradation or unavailability of functionality, recoverable without assistance; no data disclosure, no data destruction
3	Significant	Disclosure or destruction of recovered data or project files; or prolonged unavailability of a core function requiring manual recovery
4	Severe	Execution of arbitrary code on the user's machine; irreversible destruction of data; or large-scale use of the product as an attack vector affecting other devices or networks

4.4 Risk matrix and level definitions

Risk score = likelihood x impact.

Likelihood \ Impact	**1 Negligible**	**2 Limited**	**3 Significant**	**4 Severe**
4 Likely	4 Medium	8 High	12 Critical	16 Critical
3 Possible	3 Low	6 Medium	9 High	12 Critical
2 Unlikely	2 Low	4 Medium	6 Medium	8 High
1 Rare	1 Low	2 Low	3 Low	4 Medium

Risk level	**Range**	**Definition**
Low	1 to 3	Acceptable; no additional treatment required; existing controls are maintained and reviewed at the annual review
Medium	4 to 6	**Acceptable** provided the existing controls are effective and documented; improvements that are reasonable in cost should be sought and are reviewed annually
High	8 to 9	**Not acceptable.** Treatment must be defined and implemented so as to reduce the residual risk to Medium or below before the product is made available on the market

Critical	12 to 16	**Not acceptable.** Treatment must be completed before the product is placed on the market; no declaration of conformity may be drawn up until it is

4.5 Decision rule on acceptability

22. **Risk score of 6 or below (Low or Medium)**: acceptable, provided that documented controls support it, subject to review at the annual review;
23. **Risk score of 8 or above (High or Critical)**: not acceptable; the treatment decision and the residual risk must be recorded in Section 8. Once treatment is complete and verified by CRA-TR-001, the residual risk must be 6 or below;
24. Irrespective of level, **any path that could permit execution of arbitrary code on the user's machine, or irreversible destruction of user data**, must be confirmed item by item at the pre-release security gate (CRA-TD-001, Section 5.3);
25. This assessment does not "transfer" risk to the user. Where a risk can be eliminated through the design of the product itself, it may not be substituted by a warning in the user instructions.

5. Threat scenarios

Reference: Regulation (EU) 2024/2847, Article 13(2) (the results of the risk assessment are taken into account at the design, development, production, delivery and maintenance stages); Article 13(3) (risk analysis based on intended purpose and reasonably foreseeable use and conditions of use).

> *Note: The "existing controls" column records the controls **already established** in the current design and processes of the product. Where a control is marked as to be confirmed or to be verified, its effectiveness is subject to the results of CRA-TR-001. Once CRA-TR-001 has been executed, this table must be updated and the affected scenarios re-scored under the procedure in Section 10 if any conclusion changes.*

ID	Lifecycle phase	Threat / attack path	Asset affected	Existing control	Likelihood	Impact	Risk level
T-01	Design	An attacker crafts a malicious dump image exploiting an out-of-bounds read/write, integer overflow or type confusion defect in the parser to execute arbitrary	A-01, A-10	Untrusted input principle: format allow-list, header and structure validation, strict bounds checking (CRA-TD-001, Sections 3.3 and 3.4); compiler mitigation options to be confirmed (P06); malformed input and fuzz testing to be executed (CRA-TR-001, TC-05 to TC-08)	3	4	**12 Critical**

		code on the user's machine					
T-02	Design	An oversized or structurally anomalous (decompression-bomb style) dump image exhausts memory or CPU, rendering the product unresponsive	A-10	Input size limits, chunked processing, cancellable long-running tasks, persistent job state (CRA-TD-001, Section 3.4)	3	2	6 Medium
T-03	Design	A job or layout project file tampered with by a third party is loaded, triggering a parsing defect or unintended overwriting of output	A-05, A-01	Structured parsing; type and range validation of fields; file format version tagging; rejection of output paths containing path traversal fragments; confirmation before overwriting	2	3	6 Medium
T-04	Design	A maliciously crafted chip ID / configuration database file is substituted into the installation directory, disrupting parsing or triggering a parsing defect	A-04	Database files distributed with the installer; format and range validation; Perform MD5 checksum verification on the database file.	2	3	6 Medium
T-05	Design	A defect in the expression evaluator of the custom formula transformation feature causes resource exhaustion or unintended	A-01, A-10	Restricted expression evaluator with no file system, process or network access; caps on evaluation time and iteration count (CRA-TD-001, Section 3.3)	2	4	**8 High**

		operations					
T-06	Design	The product exposes unnecessary network listening ports, local sockets or debug interfaces, creating a remote attack surface	A-10	Design contains no inbound listening ports and the product does not reside as a system service (CRA-TD-001, Section 3.3); to be verified by CRA-TR-001, TC-19	1	3	3 Low
T-07	Development	Third-party open-source or commercial components (compression, imaging, cryptographic and runtime libraries) carry known vulnerabilities and are incorporated into the product (supply-chain risk)	A-01, A-10	SBOM established and updated before each release; pre-release vulnerability scanning of dependencies; preference for actively maintained components (due diligence under Article 13(5)); reporting of component vulnerabilities upstream in accordance with Article 13(6)	3	3	**9 High**
T-08	Development	Hard-coded keys, internal debug backdoors or unremoved debug interfaces are carried into the released build	A-01, A-08	Code review checklist; item-by-item confirmation at the pre-release security gate (CRA-TD-001, Section 5.3);	2	4	**8 High**
T-09	Development	The activation request carries host information or credentials beyond what is necessary, disclosing information about the	A-02, A-10	Data minimisation principle; only licence and device identifier fields are transmitted (CRA-TD-001, Section 3.4); (P07)	2	2	4 Medium

		user's device					
T-10	Build and production	The build machine or build toolchain is compromised and malicious code is injected at compile or packaging time	A-07, A-01	Controlled build environment; builds executed by a designated responsible person; build identifier written into artefacts (CRA-TD-001, Section 5.1); The build machine has no network access. (P06)	1	4	4 Medium
T-11	Build and production	The code signing private key or activation server-side keys are disclosed, copied or misused to sign malicious installers or forge activation responses	A-08, A-03	Offline generation and secure storage of secret keys.	1	4	4 Medium
T-12	Delivery and distribution	An update or installation package is tampered with in the distribution chain (third-party download sites, mirror sites, man-in-the-middle substitution) and the user installs a trojanised version	A-03, A-01	Distribution through official channels only; HTTPS throughout; published SHA-256 checksums; monotonic version number check to prevent downgrade; (P03)	2	4	**8 High**
T-13	Delivery and distribution	The official website is compromised or hijacked, or DNS is poisoned, and download links are redirected to malicious	A-09, A-03	HTTPS enabled on the website; Server data shall be backed up monthly. All system patches shall be updated to the latest version. Knowledge of passwords shall be restricted to the minimum necessary scope.	2	4	**8 High**

		files					
T-14	Delivery and distribution	The forum is used for social engineering: impersonation of the manufacturer to distribute "cracked" or "insider upgrade" packages or poisoned project files, inducing users to download and run them	A-09, A-12, A-10	Forum rules and moderation; release information published simultaneously on the website notice board and the forum; nandflashtracer@gmail.com as single point of contact with the CVD policy published (CRA-CVD-001); user information warns users to obtain the product only from official channels (Annex II, point 5)	3	3	**9 High**
T-15	Deployment and use	Activation traffic is intercepted by a man-in-the-middle, or the activation server is impersonated and a forged response returned	A-02, A-10	Outbound HTTPS only; server certificate validation; strict parsing of response fields; anomalous responses treated as failure (CRA-TD-001, Section 3.3); to be verified by CRA-TR-001, TC-12 and TC-13	2	3	6 Medium
T-16	Deployment and use	An unauthorised local person accesses an open product session and reads or exports recovered data	A-06, A-05	Reliance on the host operating system's account and file system permission model; user instructions require day-to-day operation under a standard user account (Annex II, point 8(a)); Locking function is not provided.	2	3	6 Medium
T-17	Deployment and use	Temporary files, cached images or logs created during processing remain on disk, allowing recovered personal data to be recovered by	A-06, A-11	Logs and temporary files record only what is necessary and contain no image content;	3	3	**9 High**

		others					
T-18	Deployment and use	The user's own process is inadequate (processing images containing personal data on shared or unencrypted machines, processing third-party data without authority, failing to safeguard output), resulting in unlawful data processing	A-12, A-06	User information and instructions advise processing sensitive data in a controlled, encrypted environment and state the user's responsibility as data processor (Annex II, points 5 and 8(a))	3	1	3 Low
T-19	Maintenance and update	Downgrade or rollback attack: the user is induced to install an older version containing known vulnerabilities, or weaknesses in older versions' verification are exploited	A-01, A-03	Monotonic version number check; Older software versions are not available for download from the official website. Once expired, older software versions cannot be used.	2	3	6 Medium
T-20	Maintenance and update	Activation server-side API keys or database credentials are disclosed, permitting bulk forgery of activation responses	A-08, A-02	The activation-server secret keys shall be kept with minimal access scope. Only two personnel know the backup keys. No plain- text copies are stored, hence there is no risk of leakage. Server passwords shall be changed monthly.	1	3	3 Low
T-2	Maintenance and update	The vulnerability reporting	A-12	CRA-IRP-001 incident and vulnerability reporting procedure	2	3	6 Medium

1		channel fails or the reporting chain overruns its deadlines, breaching the 24-hour early warning / 72-hour vulnerability notification / 14-day final report requirements of Article 14		established; nandflashtracer@gmail.com as single point of contact (Article 13(17)); verified by the tabletop exercise in CRA-TR-001, Section 7			
T-22	Maintenance and update	A discovered vulnerability in a third-party component or in the product itself is not remediated and released as an update within a reasonable time	A-01	CRA-VHP-001 vulnerability handling procedure with remediation deadlines set by severity; security updates provided separately from functionality updates where technically feasible; Critical 1day, High 1day, Medium 3days,Low 1week.	3	3	**9 High**
T-23	Decommissioning	User data, settings, logs and temporary files remain after uninstallation and are not permanently removed	A-06, A-11	Uninstallation route and manual deletion guidance provided (Annex II, point 8(d)); To uninstall the software, simply delete the program folder; no additional files will remain.(P15)	3	2	6 Medium
T-24	Decommissioning	The user continues to use the product after the support period ends on 10 February 2029 and no longer receives security updates	A-01, A-10	End date of the support period stated in an easily accessible manner at the time of purchase (Article 13(19));The software may be used perpetually.(P17)	3	2	6 Medium
T-2	Deployment and use	Licence circumvention and	A-02, A-12	Device binding and issue-date verification (added in the version	4	1	4 Medium

5		unauthorised redistribution (**a commercial risk to the manufacturer**; see the note below this table)		of 23 May 2025); channel management at commercial level			

Honest statement on T-25. *Circumvention of the licence and unauthorised redistribution harm the commercial interests of the manufacturer and may expose users to tampered third-party builds (that consequence is assessed separately as a user-side security risk in T-13 and T-14). As regards the product itself, however,* ***circumventing the licence check does not weaken the protection that the product affords to the confidentiality, integrity or availability of the user's data****. The manufacturer therefore does not count it as a cybersecurity risk to users under Annex I for the purposes of its conformity conclusions, and records it separately as a commercial risk to be addressed through commercial and legal channels. The manufacturer states expressly that it claims no conformity relief on account of the existence of circumvention, and that it does not rely on licence verification as a technical control for any essential requirement in Annex I.*

6. Determination of applicability of Annex I, Part I, point (2), sub-points (a) to (m)

Reference: Regulation (EU) 2024/2847, Article 13(3) (the assessment shall indicate whether and how each of the security requirements in Annex I, Part I, point (2) applies); Article 13(4) (where certain essential requirements do not apply, the manufacturer shall include clear reasons in the technical documentation).

On point (1): Annex I, Part I, point (1) requires that products with digital elements be designed, developed and produced so as to ensure an appropriate level of cybersecurity based on the risks. That requirement ***applies in its entirety*** *to this product and is implemented through the whole of this assessment (asset identification, threat modelling and risk scoring in Sections 2 to 5; the requirement-by-requirement determination and measures in Sections 6 and 7; treatment and residual risk in Section 8). The evidence is this document, CRA-TD-001 (Sections 3, 4 and 5) and CRA-TR-001.*

Sub-point	Requirement	Applicability	How it is implemented in this product	Evidence	Explicit justification where not or only partially applicable (Article 13(4))
(a)	Be made available on the market without known exploitable vulnerabilities	Applicable	SBOM established and maintained (CRA-SBOM-001); known-vulnerability scanning of dependencies before each release; malformed	CRA-SBOM-001; CRA-TR-001 (TC-01 to TC-04, TC-25); CRA-VHP-001; CRA-TD-001, Section 5.3	Not applicable: none (fully applicable)

			input testing and fuzz testing of the import/parsing path; item-by-item confirmation at the pre-release security gate that no unresolved High or Critical issue remains		
(b)	Be made available on the market with a secure by default configuration, including the possibility to reset the product to its original state	Applicable	By default no networked data processing, no telemetry, no overwriting of existing files, output directory explicitly specified by the user; a "restore defaults" route is provided and reinstallation restores the original state	CRA-TD-001, Section 3.4 and Annex A.8(a); CRA-TR-001, TC-22	Not applicable: none (fully applicable). The product is not a tailor-made product and the manufacturer has agreed no derogation from the secure default configuration with any business user
(c)	Ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to	**Partially applicable**	Implemented: security updates are provided; where technically feasible they are released as a separate revision number, separately from functionality updates; notification of available updates through the in-product "check for updates" function, the website notice board, forum announcements and email; the user may install immediately, install later or temporarily postpone;	CRA-SUP-001; CRA-VHP-001; CRA-TD-001, Section 4.3 and Annex A.8(c) and A.8(e); CRA-TR-001, TC-17 and TC-18	See Section 6.1. In summary: sub-point (c) qualifies automatic security updates with the words "where applicable"; read with recital 56, this product falls within the categories of products for which users would not reasonably expect automatic updates, and it is used in forensic and professional laboratory environments where unattended

	temporarily postpone them		security updates are free of charge. Not implemented: **automatic installation enabled by default** (see the reasoning in Section 6.1)		updating could interfere with operations
(d)	Ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access	**Partially applicable**	Implemented: licence activation and device binding verification (issue-date and device binding verification added in the version of 23 May 2025) constitutes the control mechanism governing authorised use of the product itself; local access control relies on the host operating system's account model and file system permissions, and the user instructions require day-to-day operation under a standard user account	CRA-TD-001, Sections 3.1 and 3.3 and Annex A.8(a); CRA-TR-001, TC-16	The product is a **stand-alone, single-user, locally installed desktop tool**. It provides no network service, has no inbound listening ports and no remotely or network-accessible interface, and has no multi-user account model. "Authentication, identity or access management systems" therefore have no object in this product's technical form, and there is no internal event of unauthorised access for the product to report; local unauthorised use is covered by the audit capabilities of the host operating system. As regards authorised use of the product itself, sub-point (d) is implemented

					through the device binding verification mechanism
(e)	Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means	**Partially applicable**	Implemented (other technical means): data is processed locally with no upload, no retention, no cloud processing and no telemetry; as regards transit, HTTPS (TLS) is used throughout for activation and update checking; the user instructions give guidance on enabling disk encryption and on processing sensitive data within a controlled network	CRA-TD-001, Section 3.4 and Annex A.4 and A.8(a); CRA-TR-001, TC-11, TC-14, TC-15 and TC-23	Encryption of data at rest is not applicable: the product does **not own** the data it processes. The dump images and recovered data are the user's own files, stored at file system locations chosen by the user. Product-level encryption of that data would remove the user's control over their own data and break interoperability with other forensic tools. Confidentiality of data at rest is instead assured by the disk/file system encryption mechanisms provided by the host operating system (such as BitLocker), which the product identifies and gives configuration guidance on in the user information and instructions (Annex II, point 8(a), item 3). Annex I, Part I, point (2)(e) expressly permits "or by using other

					technical means"; the product relies on local processing and non-retention as those other means
(f)	Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions	Applicable	Structure and ECC/checksum status of imported dump images are checked and corruptions reported to the user; project and configuration files are structurally validated; update packages are subject to integrity and origin verification (SHA-256; signature validity checked where code signing is used) and to a monotonic version number check; output paths containing path traversal fragments are rejected	CRA-TD-001, Sections 3.2, 3.4, 4.3 and 5.6; CRA-TR-001, TC-06, TC-09, TC-10 and TC-16	Not applicable: none (fully applicable)
(g)	Process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose (data minimisation)	Applicable	Only files explicitly selected by the user are read; no personal data is collected; activation transmits only licence and device identifier fields; no telemetry or usage statistics are returned;	CRA-TD-001, Sections 3.3 and 3.4; CRA-TR-001, TC-14, TC-15 and TC-20	Not applicable: none (fully applicable)

			logs contain no image content or personal data		
(h)	Protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks	**Partially applicable**	Implemented (local availability): input size limits, chunked processing, cancellable long-running tasks, persistent job state enabling recovery after interruption, exception handling and safe fallback, explicit error messages on import failure	CRA-TD-001, Sections 3.3 and 3.4; CRA-TR-001, TC-05, TC-07, TC-08 and TC-24	Resilience against network or remote denial-of-service attacks is not applicable: the product **provides no external service**, has no inbound listening ports, does not reside as a service and has no cloud component, so there is no network-reachable denial-of-service exposure. Availability protection is therefore implemented on the risk surface that actually exists, namely local resource exhaustion and anomalous input
(i)	Minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks	Applicable	No inbound listening ports, no residence as a service, no network scanning or broadcast behaviour, no self-propagation capability; the only network activity is user-perceptible outbound HTTPS (activation and update	CRA-TD-001, Section 3.3; CRA-TR-001, TC-19	Not applicable: none (fully applicable)

			checking)		
(j)	Be designed, developed and produced to limit attack surfaces, including external interfaces	Applicable	The attack surface is inventoried with mitigation noted for each item; the import path applies a format allow-list, structural validation, bounds checking and size limits; custom formulas use a restricted evaluator; there are no inbound listening ports or debug interfaces; the number of third-party dependencies is controlled and recorded in the SBOM	CRA-TD-001, Sections 3.3 and 3.4; CRA-SBOM-001; CRA-TR-001, TC-19	Not applicable: none (fully applicable)
(k)	Be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	**Partially applicable**	Implemented (design level): input validation and bounds checking, restricted expression evaluator, least-privilege operation, no residence as a service, no unsafe dynamic load paths. To be confirmed: compiler and linker exploitation mitigation options at binary level (ASLR, DEP/NX, control flow guard, stack protection) (P06)	CRA-TD-001, Section 5.1; CRA-TR-001, TC-04	Sandboxing or containerised isolation is not applicable: the product must perform high-throughput local I/O and memory-mapped processing of images that may reach tens or hundreds of gigabytes, and generic sandboxing would prevent its core functions from completing within acceptable time; the product does not execute untrusted code received from a network, so the

					marginal benefit of isolation is disproportionate to the functional loss. Mitigation is therefore implemented in three layers: **input validation, compiler-level exploitation mitigation, and least privilege**. The compiler mitigation options are to be confirmed; until they are, the conclusion on this sub-item is "conditionally met"
(l)	Provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user	**Partially applicable**	Implemented: a local job log is generated recording parsing tasks, errors and anomalous events, for retrospective analysis after an incident; by default the log records only what is necessary and contains no image content, recovered data or personal data; the user may adjust the log level or switch logging off in the settings (opt-out mechanism)	CRA-TD-001, Section 3.2; CRA-TR-001, TC-20	Centralised continuous monitoring and security alerting (SIEM, SOC) is not applicable: the product is an offline stand-alone tool with no server side, no multi-user account model and no network-accessible service, so there is no internal activity stream capable of being centrally monitored; establishing centralised monitoring and alerting infrastructure would also go beyond what is proportionate for a micro/small enterprise and for the risk presented

					(Article 13(2), risk-based). Sub-point (l) **expressly requires an opt-out mechanism for the user**, and the product implements that requirement directly by limiting what is recorded to the minimum security-relevant information and by giving the user the ability to switch recording off
(m)	Provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner	**Partially applicable**	Within the product's control: deletion of the settings, job and layout project files, logs and temporary files that the product itself generates (implementation status to be confirmed, P15), an uninstallation route, and guidance on manual clean-up together with a list of residual file locations. Data portability: results are exported in standard image formats for migration to other forensic or recovery systems. Outside the product's control: the user's dump images and	CRA-TD-001, Annex A.8(d); CRA-TR-001, TC-21	The product is **not** the custodian of the user's data. Dump images and recovered data are created, named, stored and owned by the user outside the product; by design the product does not retain, index or copy that data. Requiring the product to "permanently remove" files that it does not own and that the user has expressly chosen to keep would conflict both with the user's control and with the traceability requirements of forensic work. Sub-point (m) is therefore implemented as

			recovered data reside at file system locations chosen by the user; the product offers no data wiping function and the user instructions state that a reliable wiping tool should be used (Annex II, point 8(d), item 4)		follows: for data and settings generated by the product itself, a deletion route is provided; for the user's images and output, the product gives clear guidance on where they are located and on secure erasure, and retains no reference that would remain accessible to the product after uninstallation

6.1 Reasoning on sub-point (c): automatic security updates

Text of the requirement. Annex I, Part I, point (2)(c) requires products to "ensure that vulnerabilities can be addressed through security updates, including, **where applicable**, by automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, by the notification of available updates to users, and the option to temporarily postpone them". The words "where applicable" are a statutory qualifier.

Relevant wording of recital 56. Recital 56 states, in relevant part:

> *"The requirements relating to automatic updates as set out in an annex to this Regulation are not applicable to products with digital elements primarily intended to be integrated as components into other products. They also do not apply to products with digital elements for which users would not reasonably expect automatic updates, including products with digital elements intended to be used in professional ICT networks, and especially in critical and industrial environments where an automatic update could cause interference with operations. Irrespective of whether a product with digital elements is designed to receive automatic updates or not, its manufacturer should inform users about vulnerabilities and make security updates available without delay."*

Analysis as applied to this product.

26. **Nature of the product and its user base.** NFT is a **professional forensic and data recovery workstation tool** intended for professional data recovery laboratories, data recovery technicians and digital forensic bodies. Its typical users operate in controlled laboratory environments, including public-security and digital forensic bodies.
27. **Users would not reasonably expect automatic updates.** A unit of work (the parsing and reconstruction of a single chip dump) is often long-running and is typically tied to an open case or a contractual deliverable. A version change in

the middle of a job alters parsing behaviour and output format, which may affect the continuity of the job, the reproducibility of results and the traceability of the forensic chain. Users of this product therefore **would not reasonably expect** unattended automatic installation of updates, falling within the categories described in recital 56 of "products with digital elements for which users would not reasonably expect automatic updates" and of "critical and industrial environments where an automatic update could cause interference with operations".

28. **Conclusion.** On that basis, the element of sub-point (c) concerning "automatic security updates ... enabled as a default setting" **does not apply** to this product by virtue of the qualifier "where applicable". The remaining elements of sub-point (c) (vulnerabilities can be addressed through security updates, notification of available updates to users, the option to temporarily postpone them) **apply in full and are implemented**.
29. **Compensating measures.** So that the absence of automatic installation does not lengthen the window of exposure to vulnerabilities, the manufacturer implements the following compensating measures:
30. An in-product "check for updates" function and a notification of available updates at start-up;
31. Security update notices published simultaneously on the website notice board and the forum, stating the affected versions, the impact and the severity;
32. Direct email notification of users known to be affected;
33. The user's own choice of immediate installation, installation at a later time, or temporary postponement (the option to postpone);
34. Security updates provided free of charge and, where technically feasible, released as a separate revision number and not bundled with functionality updates (Annex I, Part II, point (2));
35. Where technically feasible, a notification displayed to the user in the product when the support period has ended (Article 13(19), second sentence; implementation status to be confirmed, P17).
36. **Obligations that are not reduced.** Whether or not automatic updating is used, the manufacturer must, under the final sentence of recital 56 and Annex I, Part II, point (8), continue to inform users of vulnerabilities and make security updates available without delay. That obligation is discharged through CRA-VHP-001 and CRA-SUP-001 and is in no way reduced by the partial non-applicability of this sub-point.
37. **User information and instructions.** Annex II, point 8(e) requires information on how to deactivate the default setting for the automatic installation of security updates. Since this product does not enable automatic installation by default, that information instead states that "the product does not install updates automatically; the user obtains and installs them through the in-product notification or the official download page", and explains the consequence of switching off update notifications (a longer window of exposure to known vulnerabilities).The software

does not support automatic update installation. The latest version shall be downloaded from the official FTP server.(P16)

Reference: Regulation (EU) 2024/2847, Annex I, Part I, point (2)(c); recital 56; Annex II, point 8(e); Article 13(4) and 13(19).

7. Implementation of Annex I, Part II, points (1) to (8)

Reference: Regulation (EU) 2024/2847, Annex I, Part II; Article 13(3) (the assessment shall explain how the Part II vulnerability handling requirements apply); Article 13(8).

Point	Requirement (summary)	Measures implemented in this product	Owning document / policy	Conclusion
(1)	Identify and document vulnerabilities and components contained in the product, including by drawing up an SBOM in a commonly used and machine-readable format covering at least the top-level dependencies	SBOM drawn up in SPDX 2.3 (JSON) covering at least the top-level dependencies and updated before each release; provided on reasoned request from market surveillance authorities, and available to business users and integrators on request	CRA-SBOM-001; CRA-TD-001, Section 11 and Annex A.9	Met (generation tool and storage path to be confirmed, P12)
(2)	In relation to the risks posed, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, provide new security updates separately from functionality updates	A closed loop of intake, triage, remediation, verification and release; remediation deadlines set by severity; security fixes released as a separate revision number where technically feasible, with the reasons stated in the release notice where separation is not possible	CRA-VHP-001; CRA-SUP-001; CRA-TD-001, Section 4.3	Met (remediation timetable by severity band to be confirmed)
(3)	Apply effective and regular tests and reviews of the security of the product	Security testing and review at least once every 12 months; additional testing before the release of a major version; item-by-item confirmation at the pre-	CRA-TR-001; CRA-TD-001, Sections 5.3 and 8	Met (date and conclusions of the first execution to be confirmed, P09)

		release security gate; one exercise of the vulnerability handling process per year		
(4)	Once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description, information allowing users to identify the affected product, the impacts, the severity and clear and accessible information helping users to remediate; disclosure may be delayed in duly justified cases	Notices published simultaneously on the website notice board and the forum; disclosure delayed only where the manufacturer judges the security risk of publication to outweigh the security benefit, and published promptly once users have had the opportunity to apply the patch	CRA-CVD-001; CRA-SUP-001	Met
(5)	Put in place and enforce a policy on coordinated vulnerability disclosure	A CVD policy has been adopted and published, setting out the reporting channel, response timeframes, disclosure sequencing and a commitment not to pursue good-faith reporters	CRA-CVD-001; CRA-TD-001, Section 4.2	Met
(6)	Take measures to facilitate the sharing of information about potential vulnerabilities in the product and in third-party components contained in it, including by providing a contact address for reporting vulnerabilities	nandflashtracer@gmail.com serves as the single point of contact (Article 13(17)); users may choose their preferred means of communication and are not limited to automated tools; that address is included in the user information and instructions	CRA-CVD-001; CRA-TD-001, Section 4.2 and Annex A.2	Met (URL of the page on which it is published on the website and the date of first publication to be confirmed, P01)
(7)	Provide for mechanisms to	Distribution restricted to official channels; HTTPS	CRA-SUP-001; CRA-TD-	Secure distribution

	securely distribute updates to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner	throughout; published SHA-256 checksums; monotonic version number check to prevent downgrade; code signing to be confirmed	001, Sections 4.3, 5.5 and 5.6	requirement met; the element "in an automatic manner" is **not applicable** for the reasons given in Section 6.1 and is replaced by the compensating measures of update notification plus user-confirmed installation (P03)
(8)	Ensure that, where security updates are available to address identified security issues, they are disseminated without delay, free of charge, and accompanied by advisory messages providing users with the relevant information, including on potential action to be taken	Security updates provided free of charge; notices published with each release and users known to be affected informed through the website, the forum and email; every security update released during the support period remains available for at least 10 years after its release or for the remainder of the support period, whichever is longer	CRA-SUP-001; CRA-VHP-001; CRA-TD-001, Section 4.3	Met

Note: The "effective and regular tests and reviews" required by Annex I, Part II, point (3) are, consistently with the statement on proportionality in Section 4.1, limited to verification activities that the manufacturer can carry out itself (static analysis, vulnerability scanning of dependencies, malformed input and fuzz testing, and process exercises). They do not rely on penetration testing by external firms or on third-party certification.

8. Risk treatment and residual risk

Reference: Regulation (EU) 2024/2847, Article 13(2) (minimise cybersecurity risks, prevent incidents and minimise their impact); Article 13(7).

8.1 Risks above the acceptability threshold and their treatment

Each of the risks below has an initial rating of High or Critical (score of 8 or above) and is therefore not acceptable under the decision rule in Section 4.5. Each is recorded with its treatment decision and residual risk.

ID	Initial risk	Treatment decision	Treatment measures	Owning document / verification case	Residual likelihood	Residual impact	Residual risk
T-01	12 Critical	**Mitigate**	Strengthen bounds and length checking on the import/parsing path; enable and verify compiler and linker exploitation mitigation options (ASLR, DEP/NX, control flow guard, stack protection); run malformed input testing and fuzz testing against the parsing path and create regression cases for any defects found; confirm item by item at the pre-release security gate	CRA-TD-001, Section 5.1 (P06); CRA-TR-001, TC-03, TC-04 and TC-05 to TC-08	2	3	6 Medium
T-05	8 High	**Mitigate**	Keep the restricted expression evaluator free of file system, process and network access; cap expression length, nesting depth, evaluation iteration count and evaluation time; reject and report illegal and out-of-range input	CRA-TD-001, Section 3.3; CRA-TR-001, TC-24	1	4	4 Medium
T-07	9 High	**Mitigate**	Maintain the SBOM; scan dependencies against the	CRA-SBOM-001; CRA-VHP-001; CRA-	2	3	6 Medium

			NVD and the European vulnerability database before each release; upgrade to fixed versions in preference, and where upgrade is impossible record the mitigating measure and the reasons; report upstream component vulnerabilities to component maintainers and share remediation information in accordance with Article 13(6)	TR-001, TC-01 and TC-02			
T-08	8 High	**Avoid**	Prohibit writing keys, passwords and credentials into the source code repository; run credential scanning and code review before release; released builds carry no debug backdoors or debug interfaces, as confirmed at the pre-release security gate	CRA-TD-001, Sections 5.2 and 5.3; CRA-TR-001, TC-03	1	4	4 Medium
T-12	8 High	**Mitigate**	Distribute through official channels only; HTTPS throughout; publish SHA-256 checksums; evaluate and adopt code	CRA-SUP-001; CRA-TD-001, Sections 4.3 and 5.5 (P03); CRA-TR-001, TC-16	1	4	4 Medium

			signing (Authenticode) and verify before installation; monotonic version number check to prevent downgrade; do not use third-party download sites as a source of security updates				
T-13	8 High	**Mitigate and transfer**	HTTPS on the website and least-privilege administrative account management; timely patching of the server and content management system; periodic backups with verified restorability; transfer of part of the hosting and DNS resolution security capability to the hosting provider, while retaining the ability to switch over and publish a notice rapidly in the event of an incident	The server service provider is Alibaba Cloud. Server data is backed up on a monthly basis.	1	4	4 Medium
T-14	9 High	**Mitigate**	Forum rules prohibit posting of cracks and third-party installers, with prompt moderation; the website notice board and the forum publish release	CRA-CVD-001; CRA-TD-001, Annex A.2, A.5 and A.8(a)	2	3	6 Medium

			and security notices simultaneously; the single point of contact and the CVD policy are published on the website; rapid public clarification and notice where impersonation is detected				
T-17	9 High	**Mitigate**	Confine temporary files and cached images to the application data directory with restricted access permissions; minimise residence time and clear them at the end of a job or on exit; logs record no image content, recovered data or personal data; state in the user instructions the default location of temporary and cached files and how to clear them	CRA-TR-001, TC-20 and TC-21; CRA-TD-001, Annex A.8(d)	2	3	6 Medium
T-22	9 High	**Mitigate**	Establish remediation deadlines by CVSS severity band; provide security updates separately from functionality updates where technically feasible; keep every security update released during the support period	CRA-VHP-001; CRA-SUP-001	2	3	6 Medium

			available for at least 10 years or the remainder of the support period, whichever is longer; report annually on vulnerability disposition				

8.2 Risks not exceeding the threshold

The threat scenarios rated Medium or Low (score 4 to 6 or 1 to 3) - T-02, T-03, T-04, T-06, T-09, T-10, T-11, T-15, T-16, T-18, T-19, T-20, T-21, T-23, T-24 and T-25 - are **acceptable** under the decision rule in Section 4.5. The treatment decision for them is **accept and maintain the existing controls**, subject to review at the annual review. Two of them are noted specifically:

38. **T-25 (licence circumvention and unauthorised redistribution)**: the treatment decision is **accept**, addressed as a commercial risk through commercial and legal channels. The manufacturer does not rely on licence verification as a technical control for any essential requirement in Annex I and claims no conformity relief on that basis (see the note below the table in Section 5).
39. **T-18 (inadequate process on the part of the user)**: the treatment decision is **accept and continue to inform**. The risk arises from the autonomous conduct of the user as data controller and is outside the manufacturer's control. The manufacturer reduces its likelihood through clear warnings in the user information and instructions (Annex II, points 5 and 8(a)), but information to users may never be used as a substitute for technical treatment within the product itself.

8.3 Acceptance of residual risk

40. After the treatment in Section 8.1, **all residual risks are reduced to 6 or below (Medium or Low)** and therefore fall within the acceptability range set in Section 4.5;
41. For items whose residual risk is Medium, the effectiveness of the controls is subject to the results of CRA-TR-001. If a control is shown to be ineffective, that risk must be re-scored and retreated under the Section 8 procedure;
42. The manufacturer does not accept any residual risk rated Critical or High into the release process. If a High or Critical risk cannot be reduced to 6 or below before release, the manufacturer will postpone making that version available on the market until treatment is complete.

9. Conclusions of the assessment

Reference: Regulation (EU) 2024/2847, Article 13(2), (3) and (4); Annex VII, point 3.

43. **Overall risk level: Medium (manageable).** The overall cybersecurity risk level of the product at the assessment baseline version Ver 2.26.8 is rated **Medium**. This conclusion rests on the following: the effective attack surface is concentrated in

the local file import and parsing path; the product has no inbound listening ports, no cloud component and no remote data processing; and after the treatment in Section 8 all residual risks fall within the acceptable range (score of 6 or below).

44. **On "made available on the market without known exploitable vulnerabilities" (Annex I, Part I, point (2)(a)).** The manufacturer declares that the product, as made available on the market, contains no known exploitable vulnerabilities. That declaration is supported by the dependency inventory in CRA-SBOM-001, pre-release vulnerability scanning of dependencies, static analysis, malformed input and fuzz testing (CRA-TR-001), and by the pre-release security gate (CRA-TD-001, Section 5.3). **The declaration takes effect once CRA-TR-001 has been executed and it has been confirmed that no unresolved High or Critical issue remains.** Before the tests have been executed, the conclusion is "conditionally established".
45. **On taking the results into account across the lifecycle phases (Article 13(2)).** The results of this assessment have been taken into account and implemented as follows:
46. **Planning and design**: threat scenarios T-01 to T-06 directly drove the design decisions on bounds checking on the import/parsing path, input size limits, the restricted expression evaluator and "no inbound listening ports" (CRA-TD-001, Sections 3.3 and 3.4);
47. **Development**: T-07, T-08 and T-09 drove third-party component due diligence, SBOM maintenance, keeping credentials out of the repository, and the data minimisation principle;
48. **Production (build and packaging)**: T-10 and T-11 drove the controlled build environment, writing of the build identifier and the pre-release security gate;
49. **Delivery and distribution**: T-12, T-13 and T-14 drove the restriction to official channels, HTTPS transport, publication of checksums and the monotonic version number check;
50. **Deployment and use**: T-15 to T-18 drove certificate validation on the activation channel, minimisation of logs and temporary files, and the information given in the user information and instructions;
51. **Maintenance and update**: T-19 to T-22 and T-24 drove the vulnerability handling procedure, remediation deadlines by severity band, free provision of security updates and the end-of-support notification;
52. **Decommissioning**: T-23 drove the uninstallation guidance, the list of residual files and the recommendation on secure erasure.
53. **On the applicability of the essential requirements.** Of sub-points (a) to (m) of Annex I, Part I, point (2), six - (a), (b), (f), (g), (i) and (j) - apply in full; seven - (c), (d), (e), (h), (k), (l) and (m) - are partially applicable, and the non-applicable elements together with the explicit reasons are recorded in Section 6 in accordance with Article 13(4). Annex I, Part I, point (1) applies in its entirety. All of points (1) to (8) of Annex I, Part II are implemented.
54. **On harmonised standards.** As at the date of this document (2 September 2026), no reference to a harmonised standard under the CRA has been published in the

Official Journal of the European Union, and the standards commissioned from CEN/CENELEC/ETSI under standardisation request M/606 are still under development. The manufacturer therefore **does not claim the presumption of conformity under Article 27**, and the product is assessed directly against the essential requirements in Annex I. The EN 18031 series is a set of standards supporting the Radio Equipment Directive and is unrelated to this Regulation; it is not cited.

10. Update and maintenance of the assessment

Reference: Regulation (EU) 2024/2847, Article 13(3) (the risk assessment shall be documented and kept up to date during the support period); Article 13(7) (systematic recording of relevant cybersecurity matters and updating of the risk assessment as appropriate); Article 13(13).

10.1 Period of maintenance

This assessment is maintained and updated as appropriate at least throughout the support period, **10 February 2024 to 10 February 2029**. The support period is determined under Article 13(8) and the information taken into account in determining it is set out in CRA-TD-001, Section 6.

10.2 Triggers for update

On the occurrence of any of the following, the manufacturer shall initiate an update of this assessment within 30 days :

55. **A new vulnerability is discovered**: in the product itself or in one of its third-party components, in particular an actively exploited vulnerability or a vulnerability of high severity;
56. **A security incident occurs**: an incident affecting the product, or a vulnerability or severe incident reported under Article 14;
57. **A substantial modification**: the product undergoes a substantial modification within the meaning of Article 3, point (2) (affecting its compliance with the essential requirements in Annex I, Part I, or changing the intended purpose for which it was assessed), including a major change to import formats, the parsing engine, the activation mechanism, the update mechanism or third-party dependencies;
58. **The operating environment changes**: a change in the range of supported operating system versions, a change in the security mechanisms of the host environment, or the emergence of a new reasonably foreseeable use;
59. **A new harmonised standard or common specification appears**: a reference to a harmonised standard under the CRA is published in the Official Journal of the European Union, or common specifications under Article 27 or a European cybersecurity certification scheme are adopted on which the manufacturer intends to rely for a presumption of conformity;
60. **The threat landscape changes materially**: publicly available attack techniques emerge against comparable products or comparable parsing paths;

61. **A control fails**: CRA-TR-001 shows that a control is ineffective or only partially effective;
62. **A compliance document changes**: the SBOM content, the vulnerability handling procedure, the update distribution channel or the single point of contact changes.

Note: Updates to this assessment are kept consistent with CRA-TD-001, Section 1.6 (triggers for re-assessment) and Section 12.3 (change triggers); the two are revised together.

10.3 Record-keeping

63. The manufacturer systematically records relevant cybersecurity matters in a manner proportionate to the nature and risks of the product, including vulnerabilities of which it is aware and information provided by third parties, and updates this assessment as appropriate (Article 13(7));
64. Those records include: vulnerability reports and intake records; triage and disposition records; test execution records and results; update release records; reporting and communication records; and the version history of this assessment;
65. As part of the technical documentation, this assessment is kept **for at least 10 years after the product has been placed on the market or for the support period, whichever is longer**, and is made available to national authorities on request (Article 13(13));
66. This document is located on the “About” page of the official website.(https://www.flash-tracer.com/about.html) (P14).

11. Items pending confirmation

*Note: The placeholders below are replaced with the actual content once the corresponding matter is confirmed, and the conclusions and risk ratings of the affected sections are updated at the same time. Until a placeholder is closed, the corresponding conclusion in this document is **conditionally established**, and the treatment of High and Critical risks may not be regarded as complete.*

No.	Placeholder	Section	Note
P04	NFT-2.26.8.26-20260826	2.1	Number carried over from CRA-TD-001; product identification element under Article 13(15)
P03	-	5 (T-12), 6 (c)(f)(k), 7 (7), 8.1	Number carried over from CRA-TD-001; affects the residual risk of T-12
P06	MSVC(Visual Studio 2022) 19.38 Protected by software packing. The protection software and its version are not publicly available for the time being.	5 (T-10), 6 (k), 8.1	Number carried over from CRA-TD-001; affects the residual risk of T-01 and T-10
P07	Domain name: www.flash-tracer.com	5 (T-09), 6 (g)	Number carried over from CRA-TD-001; basis for

	Field content: Activation Code		the data minimisation determination
P15	No uninstall entry is provided for the software.	5 (T-23), 6 (m)	Number carried over from CRA-TD-001; affects the conclusion on sub-point (m)
P16	Automatic installation and update are not applicable.	5 (T-19), 6.1, 6 (c)	Number carried over from CRA-TD-001; requirement of Annex II, point 8(e)
P17	A prompt will be displayed upon software startup when the license expires.	5 (T-24), 6.1	Number carried over from CRA-TD-001; Article 13(19), second sentence
P01	https://www.flash-tracer.com/about.html	7 (6)	Number carried over from CRA-TD-001; evidence requirement of Annex VII, point 2(b)
P12	ftp://bytesmart@www.flash-tracer.com	7 (1)	Number carried over from CRA-TD-001
P09	Test date: August 27, 2026. Test result: Passed.	8.1, 9	Number carried over from CRA-TD-001; the validity of residual risk depends on the test results
P14	The text is stored on the local server at D:\TestResult. The responsible person for access is Jin Cancan. Incremental backup is adopted.	10.3	Number carried over from CRA-TD-001; Article 13(13)
RA-01	MD5 verification is applied to database files.	5 (T-04)	Affects the effectiveness of the control for T-04
RA-02	No	5 (T-08)	Affects the treatment measures for T-08
RA-03	The build machine is not connected to the network.	5 (T-10)	Affects the effectiveness of the control for T-10
RA-04	The computer used for key generation and storage is not connected to the network.	3 (A-08), 5 (T-11, T-20)	Affects the criticality of A-08 and the

			effectiveness of the controls for T-11 and T-20
RA-05	Person-in-charge: Zhou Yang	3 (A-03, A-09), 5 (T-13, T-14)	Owner column of the asset register
RA-06	Publication of content on the official website and forum requires administrator review. Server permissions are held only by the person-in-charge and the administrator. Server content is backed up monthly, and user data is backed up incrementally. The hosting service provider is Alibaba Cloud.	5 (T-13), 8.1	Affects the residual risk of T-13
RA-07	Cache files are placed at the same directory level as image files. They are destroyed after use. File permission management is not required upon exit.	5 (T-17), 6 (m), 8.1	Affects T-17 and the conclusion on sub-point (m)
RA-08	No locking interface needs to be provided.	5 (T-16)	Affects the conclusion on sub-point (d)
RA-09	No download links for older-version installation packages are provided. Outdated software packages cannot be executed.	5 (T-19)	Affects the effectiveness of the control for T-19
RA-10	Critical 1 day, High 1 day,Medium 3 days, Low 1 week.	5 (T-22), 7 (2), 8.1	Affects the treatment measures for T-22
RA-11	Internal deadline for initiating an update of this assessment after a trigger 30 days.	10.2	Executability of the update process
RA-12	Finalization date: September 3, 2026. Risk level: No risk.	Throughout	Corresponds to item P10 in CRA-TD-001

Signature record

Role	Name	Signature	Date
Prepared by	Jin Cancan		2 September 2026
Reviewed by	Zhou Yang		2 September 2026
Approved by	Zhou Yang		2 September 2026