



Four completeness rules — written, tested over 24 months, costed

LINDBERGH FORMATION — 16 rue de Maillé, 91310 Montlhéry, France · Companies register (RCS) Evry 817 946 114

Document issued on 24/09/2026

Run over 2,920 reports received between 1 January 2024 and 31 December 2025 · fictional document

Fictional document — demonstration example

This document is produced by the Blue Lemon Agent website to illustrate what an AI agent hands to its users. The companies, matters, amounts and people in it are invented. It has no legal, accounting or commercial value.

Fictional document, produced for the demonstration. **None of these rules is in force: they are written, measured and put on the table. A rule only enters service once the head of the inspection unit has validated it. They bear on the FORMAL COMPLETENESS of a report — never on its merits, which are for the inspector.**

The four rules, with what each raises and what it lets through

Rule	What it raises	Flags over 24 months	Confirmed on examination	Reliability

A	Report without workable identification of the establishment (company name + company number, or company name + address)	486	471	96.9 %
B	Report with no date or period of the facts	402	381	94.8 %
C	Report concerning a named person, without their job or length of service	264	222	84.1 %
D	Document announced in the body of the report, absent from the file 15 days after the acknowledgement	218	196	89.9 %
Together	Distinct incomplete files covered	1,370 flags	1,124 distinct files	93.0 % of the 1,208

Why 1,370 flags make only 1,124 files: the same report often triggers two rules — typically A and B. **The figure that matters to you is distinct files, not alerts**, and that is the one carried into the year-in-review.

What the first three let through — and why rule D was written

218 reports were complete under rules A, B and C: establishment identified, period bounded, person placed. **All of them announced a supporting document — a payslip, a rota, a message thread — that never arrived.** None of the first three rules saw them, and yet they are the most frustrating files: **they look workable right up to the moment the inspector opens the document and cannot find it. Rule D raises the gap 15 days after the acknowledgement, which is still within the window in which the person who filed the report replies.**

The qualified acknowledgement of receipt — the proposed wording, to be settled

Situation detected	What the acknowledgement tells the person who filed	What it does not say
Establishment not identifiable	The missing item named, where to find it (payslip, contract, letter from the employer), and the time allowed to bring it	Nothing on the merits of the report
Facts undated	A request for the period, with an example of accepted wording	No assessment of seriousness
Person not placed	A request for the job held and length of service, and why it changes the handling	No promise as to follow-up
Announced document not received	A reminder of the announced document, the time remaining, and the channel to send it	No judgement on the document's absence

Rules A / B / C / D brought into service by the head of the inspection unit, on: _____

What bringing them into service changes, in figures: of the year's **604 incomplete reports, 562 would have received their qualified acknowledgement within the minute instead of a request for further information at 21 days. That is not a time saving for the unit, it is a delay saving for the person who wrote in** — and for the files that, today, never come back.

Scope of this document: the service operated by Blue Lemon Agent. For an agent deployed at your premises, the applicable location is that of the architecture set out in the quotation and verified before commissioning; local execution is announced only for the configuration explicitly described and accepted in the quotation; the applicable isolation depends on the deployment mode set out in the quotation, no dedicated isolation being presumed; the encryption mechanisms in transit and at rest, their components and key management are those documented for the architecture chosen; roles and permissions are configured and accepted for the identities and systems actually connected; the events logged, their content, their retention period and who may access them are defined for the deployment chosen.