

How to prepare a business for an audit without disrupting operations

[Czytaj po polsku](#)

Agree scope, authorisation, records and report acceptance before work begins.

Prepared by DATPOL, 4 October 2026. This guidance supports scoping, discussions and acceptance; it does not replace a design or the specific equipment manual. This British English version concerns services and properties in Poland.

Define the question the audit must answer

Is the focus installation reliability, IT security, physical protection or an upgrade? Identify sites and processes. Put any specific compliance criteria in scope: a general review does not automatically establish compliance.

Separate inspection from active testing

Agree document access, interviews and visual inspections. Scanning, penetration testing, isolation and failure simulations require defined authorisation, a work window and stop conditions. Permission for an audit is not permission for every intervention.

Accept an action plan

The report should connect each observation with evidence, impact and a recommendation. Ask for priorities, action owners and a distinction between urgent repairs and capital work. Ensure assessment limitations are recorded.

Practical checklist

- Objective, sites and scope.
- Records and interview contacts.
- Authorisation and testing limits.
- Report format and follow-up verification.

Next steps and references

[DATPOL service scope and supporting material](#)

Support requests: [DATPOL24](#). Do not include passwords or secrets in the form.

Related guides

- [How to compare an indoor server room with a container solution](#)
- [What to prepare before connecting a public authority to a SOC](#)
- [How to document a backup recovery test](#)

Revision #2

Created 2026-10-04 14:56:34 UTC by Administrator DATPOL

Updated 2026-10-04 14:56:35 UTC by Administrator DATPOL