

What to prepare before connecting a public authority to a SOC

[Czytaj po polsku](#)

Inventory, log sources, authorisation and response testing before service acceptance.

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.

Describe the environment and owners

List sites, systems, servers, endpoints, network devices and suppliers. Identify owners and critical services.

Agree log sources, time synchronisation and secure transfer. No events may indicate a missing integration rather than absence of threats.

Agree response authority

Record contact channels, service hours, priorities and actions needing approval. Automated blocking can interrupt work, so it needs an approved rule, exceptions, an audit trail and an unblock procedure. An alert is not the same as a confirmed intrusion.

Test the whole event workflow

Using an agreed scenario, test event delivery, detection, notification and documented response. Accept a list of active integrations and gaps. A SOC supports detection and response; it does not replace risk management, backups or all of an organisation's obligations.

Practical checklist

- Inventory and critical services.
- Log sources and delivery tests.
- Contacts, escalation and approved actions.
- Acceptance record and outstanding gaps.

Next steps and references

[DATPOL service scope and supporting material](#)

[CISA — Use Logging on Business Systems](#)

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

Related guides

- [How to prepare a business for an audit without disrupting operations](#)
- [How to compare an indoor server room with a container solution](#)
- [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