The DLP Program Health Check Checklist

25 questions to determine whether your DLP program is protecting data or just generating alerts.

HOW TO USE IT

Mark Yes, Partial, or No. Any cluster of Partial or No answers is a good candidate for a focused review.

		YES	PARTIAL	NO
TOOL COVERAGE				
01	Are email, endpoint, USB, web upload, cloud, and collaboration channels covered by enforceable controls?	☐	☐	☐
02	Are inspection points aligned to the data flows that matter most to the business?	☐	☐	☐
03	Are known blind spots documented with owners and risk acceptance?	☐	☐	☐
POLICY MATURITY				
04	Do policies map to clear data classes, business use cases, and regulatory drivers?	☐	☐	☐
05	Is rule logic precise enough to catch high-risk movement without over-blocking routine work?	☐	☐	☐
06	Are rules reviewed on a set cadence after incidents, workflow changes, or new tools?	☐	☐	☐
AGENT HEALTH				
07	Can you report deployment coverage by device, user group, operating system, and business unit?	☐	☐	☐
08	Are unhealthy, outdated, or disabled agents surfaced and remediated quickly?	☐	☐	☐

Checklist continued

Use the answers to identify control gaps, tuning opportunities, and the workflows where DLP should be easier for analysts and business users to trust.

		YES	PARTIAL	NO
ALERT QUALITY				
09	Which rules generate the highest alert volume, and why?	☐	☐	☐
10	Can analysts separate true positives from noisy patterns without manual guesswork?	☐	☐	☐
11	Are false-positive sources tracked to specific rules, data patterns, or workflows?	☐	☐	☐
EXCEPTIONS				
12	Are exceptions time-bound, justified, and reviewed by the right owner?	☐	☐	☐
13	Do bypasses include compensating controls, monitoring, or documented risk acceptance?	☐	☐	☐
CLASSIFICATION				
14	Do classification labels match how sensitive data is actually created, stored, and shared?	☐	☐	☐
15	Are detection methods tested against real examples and edge cases?	☐	☐	☐
16	Is classification drift measured when business processes or repositories change?	☐	☐	☐
INCIDENT RESPONSE				
17	Does the triage workflow define severity, evidence, containment, and escalation criteria?	☐	☐	☐
18	Are DLP events linked to incident response playbooks for exfiltration or policy-violation scenarios?	☐	☐	☐

Checklist continued

Finish the review by checking whether reporting, business workflow impact, and ownership are clear enough to drive action.

		YES	PARTIAL	NO
REPORTING				
19	Do dashboards show risk reduction, not just alert volume?	☐	☐	☐
20	Can leaders see coverage, high-risk gaps, policy performance, and trend movement?	☐	☐	☐
BUSINESS WORKFLOWS				
21	Are high-friction controls mapped to the business processes they affect?	☐	☐	☐
22	Are users given safe alternatives when risky movement is blocked or coached?	☐	☐	☐
23	Do policy changes account for productivity impact and exception demand?	☐	☐	☐
OWNERSHIP AND GOVERNANCE				
24	Is ownership clear across policy tuning, investigations, approvals, and reporting?	☐	☐	☐
25	Is there a 30/60/90-day roadmap tied to measurable control improvement?	☐	☐	☐

NEXT STEP

If several answers are Partial or No, the DLP Program Health Check turns those signals into prioritized findings, alert-noise reduction opportunities, and a 30/60/90-day improvement roadmap.

hello@controlwrightcyber.com

controlwrightcyber.com