

Production Continuity Checklist

A ransomware production shutdown doesn't require touching a single machine on the plant floor. This worksheet tests the question most protection-focused programs never ask: what can your plant still execute when the systems supporting it are unavailable.

FACILITY / LINE

DATE

REVIEWED BY

01 Critical production processes

Which processes, if halted, stop shipping product entirely — not merely slow it down?

02 Supporting IT dependencies

For each critical process above, which IT-side systems does it require to run (ERP, MES, scheduling, quality release, dispatch)?

03 Single points of coordination

Which of those systems, if unavailable, stall more than one process at once? These are the load-bearing nodes.

04 Manual / degraded capability

Has anyone actually run the process manually — not assumed it's possible?

05 Identity dependencies

Which processes require a corporate identity provider that may not survive the same incident?

06 External / cloud dependencies

Which coordination systems live outside the plant network entirely (cloud ERP, hosted scheduling)?

07 Recovery-window assumptions

What's the realistic recovery window for each dependency above — and is it documented or assumed?

08 Production-to-recovery handoff

Who decides when to switch from manual/degraded operation back to system-coordinated operation, and how is that decision made?

09 Last tested date

When was this degraded-operation capability last actually tested, not just discussed?

10 Owner

Who owns keeping this answer current as systems and processes change?