Centribolt

Identity Evidence Self-Check

Can you show that a privileged access control is working, today, without starting a project?

How to use this checklist

Pick **one privileged access control at a time**, for example domain administrator accounts or local administrator accounts on servers.

Answer **Yes** only if you can show the evidence today. Answer **Partly** if it exists but is incomplete or out of date. Answer **No** if it does not exist or you cannot show it.

No.	Check	Yes	Partly	No
1	A register lists the privileged accounts in scope, with the date it was last updated.			
2	Each account has a named owner recorded.			
3	Each account has a recorded business purpose.			
4	The approval for each account's access is on record, with the date and the approver.			
5	The last access review is on record: date, reviewer and outcome.			
6	Changes since that review (accounts added, removed or changed) are on record.			
7	Use of privileged access is logged for the systems in scope.			
8	Log retention is defined, and logs can be retrieved for a given account and date.			
9	Accounts outside the control are listed, each with a reason, an owner and an expiry date.			
10	Accounts of people who have left are shown as removed, with the removal date.			
11	The register has been compared with the environment itself, using each system's own account list, and the date of that comparison is recorded.			
12	The control owner can produce items 1 to 11 on request, without starting a project.			

What to do with the answers

Every No or Partly is a finding. Give each one a named owner and a date.

Start with the lines that affect the most accounts or the least-reviewed systems. A control that has an owner but no evidence is easier to fix than one with neither.

Repeat the check for the next control, and repeat it for the same control after changes.

An Excel version of both checklists, with a summary tab, is on the Resources page at centribolt.com/resources.html.

Need an independent view? Request an Identity Security Posture Review at centribolt.com/contact.html. A mutual non-disclosure agreement comes first if you want one.

General guidance for self-assessment. It is not legal, audit or compliance advice, and answering Yes to every line does not mean any standard or regulation is met.