

ccTLD Hijack Recovery Checklist

A compact, printable checklist for reviewing certificate exposure and confirming issuance controls after controls after authoritative DNS recovery.

ORDER: 01 AND 02 START AT ONCE · 03 BEFORE 04 · 05 CLOSES THE WORKSTREAM

01	Inventory all affected domains Include parked domains and regional ccTLDs. Build the list from registrar and registrar and registry records, not from memory. RECORD Domain list, record source per domain, scope decision	☐ DONE OWNER _____ DATE _____
02	Review Certificate Transparency logs Search CT for every inventoried domain. Flag any certificate you cannot trace to known issuance. RECORD Search date, window covered, certificates flagged, reviewer	☐ DONE OWNER _____ DATE _____
03	Verify authoritative DNS control is restored Confirm from outside your network that the delegation and each authoritative server return the expected records. RECORD Delegation as served, answers per authoritative server	☐ DONE OWNER _____ DATE _____
04	Verify restrictive CAA policy and CA support Confirm the restored servers return your CAA policy and each authorized CA supports the restrictions you rely on. RECORD CAA as served; CA support documentation per restriction	☐ DONE OWNER _____ DATE _____
05	Record evidence before closing Attach the evidence from checks 01 to 04, name an owner and list open items. Close only the issuance recovery workstream. RECORD Dated evidence file, named owner, open items carried forward	☐ DONE OWNER _____ DATE _____

BOUNDARY: WHAT PASSING THESE CHECKS DOES NOT SHOW

Passing all five checks does not revoke any certificate already issued and does not show that no unauthorized certificate exists. Restored DNS is necessary, but it is not sufficient evidence that issuance is back under control. Existing certificate exposure, revocation status and residual risk need separate investigation.