CROSS-PILLAR · FIELD NOTES

The Containment Boundary Is Moving

What ICANN's DNS abuse policy shift means for your domain portfolio portfolio

One Report. One Domain. One Decision.

Since April 2024, ICANN's Registrar Accreditation Agreement obligates obligates registrars to act on exactly one thing: the single domain named in an named in an abuse report.

Nearly 530 investigations opened. Over 25,000 domains mitigated — one at a time.

Coordinated Abuse Runs on Portfolios, Not Domains

Phishing kits and malware campaigns run on dozens of domains registered registered through the same account. Mitigate one, and the campaign just campaign just stops using that domain — the operator loses nothing that nothing that mattered.

Associated Domain Checks: Proposed, Not Settled

PROPOSED — NOT A RULE

GNSO working group deliberating since ICANN85/86. Trigger threshold and sequence still unresolved. Target Initial Report: February 2027.

CHECK 1 OF 5

Registrant of Record

Who is the registrant on every domain your organization holds — not who manages it operationally, but whose name and account it sits under.

CHECK 2 OF 5

Shared Signals

Which domains share a registrant email, account login, or billing relationship — including ones acquired through M&A or picked up by an agency years ago.

CHECK 3 OF 5

Dormant Coupling

Which domains are dormant but still technically active — and still coupled to a live account.

CHECK 4 OF 5

Third-Party Control

Which agencies, resellers, or former employees retain administrative control over any domain in the portfolio.

CHECK 5 OF 5

Exposure Signal

Where a single compromised credential or account signal would create exposure across more domains than anyone tracking incident response actually knows about.

Map Your Account-Level Footprint Before ICANN Forces the Question

rack2cloud.com | Follow The Architect for more