

NEWS – ECIPE PRESS RELEASE – NEW POLICY BRIEF

Cloud Resilience and Security: Why Exit, Portability, and Lifecycle Design Matter

By **Matthias Bauer** and **Dyuti Pandya**, *Director and Analyst at ECIPE, respectively*

Brussels, 12 February 2026 - A new [Policy Brief](#) shows that **cloud resilience is a lifecycle challenge that depends on early design, licensing, and integration choices** that determine whether organisations can later adapt, switch providers, or recover from disruption. Concentration becomes a systemic risk when those choices restrict portability, interoperability, and practical exit in real-world operations.

The most important constraints are set at onboarding. **Licensing frameworks and contractual** terms determine which applications and security tools can be deployed, whether workloads can be duplicated, migrated, or dual-run, and whether recovery and substitution remain operationally viable under stress. While technical interoperability remains challenging in complex cloud environments, switching and diversification are often blocked primarily by commercial and legal constraints rather than by technology alone.

Restrictive practices used by cloud providers – including limits on **licence mobility, discriminatory pricing across clouds, and forced re-purchase during migration** – can convert scale into structural dependency. **Effective policy should therefore prioritise removing contractual and licensing barriers to lifecycle choice, rather than attempting to redesign cloud architectures through technical mandates.**

“Licensing practices may contribute to market concentration, but their more significant effect is limiting contestability – restricting customers’ ability to switch providers or combine services across multiple clouds, thereby weakening customer choice and reducing the resilience benefits that multi-cloud strategies are meant to deliver”, says Matthias Bauer, co-author of the study”, says Matthias Bauer, co-author of the study.

The brief also cautions that applying platform-style technical rules to cloud services and treating geographical sovereignty as a substitute for user resilience will **narrow multi-cloud choice**.

Overall, effective cloud resilience policy should:

- **prioritise licensing portability and neutrality**, allowing existing software entitlements to move freely across cloud environments;
- **prevent discriminatory pricing and forced re-purchase** when workloads are migrated or run in parallel across providers;
- **preserve the ability to deploy independent applications and security tools**, not only provider-native services;
- **focus competition enforcement on practical switching and exit**, not on market shares alone; and
- **avoid prescriptive technical mandates that narrow architectural diversity** and increase correlated failure risks.

Publication details: [Cloud Resilience and Security: Why Exit, Portability, and Lifecycle Design Matter](#), ECIPE Policy Brief No. 03/2026

Contact the corresponding author: Matthias Bauer, matthias.bauer@ecipe.org

Media inquiries: info@ecipe.org or +32 (0)499 053 110