Microsoft Sovereign Resilience

WHAT IT IS

A Microsoft-native resilience offering that enables critical infrastructure, SaaS, Data & AI workloads to remain **operational, compliant, and under customer control** as sovereign, regulatory, or geopolitical constraints escalate. It extends BCDR to cover scenarios where recovery is technically possible but **legally or operationally blocked**, using pre-approved degradation, identity and key survivability, and tiered sovereign operation.

KEY COMPONENTS

- **Microsoft-native architecture** across Sovereign Azure, Azure Local, and Microsoft SaaS
- **Resilience and exit designed per critical workload**, not assumed for the whole IT estate
- **Clear operating modes** for different resilience scenarios
- **Identity, access, and encryption keys** that continue to work under constraint
- **Dependencies awareness**, with approved and lawful ways to continue in reduced mode
- **Operational resilience aligned to regulation**, including DORA, & NIS2
- **Pre-defined response scenarios** for loss of control, legal separation, forced isolation, and return to public cloud

WHY IT MATTERS

A workload that only survives provider outage is not sovereign.

Under sanctions, legal restriction, or loss of control, availability alone fails.

Sovereign resilience ensures the **Minimum Viable Business** continues lawfully, decision authority is retained, and outcomes are controlled—avoiding panic-driven exits and making strategy executable under pressure.

OUTCOMES

- Lawful continuity of the Minimum Viable Business under sovereign constraint
- Pre-approved resilience and exit paths executable without crisis redesign
- Board- and regulator-defensible sovereign resilience posture, per workload