M365 BreakGlass Maturity Model

GitHub.com/KuShuSec v1.1

Unprepared	No breakglass account or app.
	No documented recovery process.
	Breakglass = “hope it never happens.”
Reactive	Breakglass account exists but rarely tested.
	App registrations are unmanaged and unmonitored.
	Secrets stored in plain text or left to expire unnoticed.
	Application Admin is assigned permanently to a few users.
	Offline credentials (e.g., passphrase or QR) stored in secure location.
Baseline Hygiene	App secrets tracked manually; redirect URIs reviewed occasionally.
	Some use of PIM for privileged roles.
	App Admin role assignments starting to be reduced.
	Breakglass CA exclusions are tightly scoped — only exclude policies that may block emergency recovery (e.g. device state), but maintain sign-in risk or location checks where feasible.
Controlled	Application Admin role only PIM-eligible with approval workflows.
	Privileged role assignments reviewed via Access Reviews.
	Consent grants require admin approval.
	Breakglass account uses FIDO2/passkey backed MFA.
	Secrets have defined expiry; basic automation for renewal exists.
	Redirect URIs are strictly scoped.
	Monitoring for service principal logins is in place.
Secure by Design	All workload identities use Workload Identity Federation (WIF).
	Secrets/certs fully automated via key vault or secure pipelines.
	Workload identity Conditional Access policies enforced.
	Entra Workload ID Premium licensing applied universally.
	Alerts for anomalous app behavior integrated into SIEM/SOAR.
	Recovery procedures are documented, tested quarterly.
	Breakglass application exists with clear scoping.
	Adversary emulation (e.g., purple team) used to validate response.
	Recovery planning accounts for Microsoft service outages, misconfigurations, and attacker scenarios.
Automated & Resilient	Entire breakglass app process is policy-as-code, version-controlled.
	All privileged app access paths are just-in-time and require approval.
	RBAC, CA, identity protection, and detection rules applied to workload identities just like user identities.
	Continuous posture monitoring via Defender for Cloud or Entra Identity Governance.
	Disaster recovery simulation of breakglass scenario part of regular purple team exercises.
Isolated Resilience	Breakglass identity/app hosted in external (red) tenant.
	Red tenant identity has just-in-time access into primary tenant via B2B or B2B Direct.
	Red tenant identity protected with independent security stack.
	Offline access credential backup exists (QR code, physical token, etc).
	Breakglass identity or app optionally backed by alternate identity provider or tenant to avoid dependency on primary cloud platform.