# Checklist Kesiapan Backup Menghadapi Ransomware

Gunakan checklist ini untuk menilai kesiapan backup anti-ransomware Anda.

- [ ] **1. Apakah data dan sistem kritis sudah dipetakan?**
  Database, aplikasi, konfigurasi, mesin virtual, email, dan data keuangan
- [ ] **2. Apakah urutan pemulihan sudah ditentukan?**
  Kelompokkan sistem: kritis, tinggi, menengah, dan rendah
- [ ] **3. Apakah tersedia lebih dari satu salinan backup?**
  Tidak bergantung pada satu media atau satu perangkat penyimpanan
- [ ] **4. Apakah salah satu salinan disimpan di lokasi berbeda?**
  Backup offsite melindungi dari kebakaran, banjir, atau pencurian
- [ ] **5. Apakah tersedia salinan offline atau immutable?**
  Salinan yang tidak bisa dijangkau, diubah, atau dihapus ransomware
- [ ] **6. Apakah akun backup dipisahkan dari admin harian?**
  Akun khusus pengelola backup, terpisah dari akun kerja rutin
- [ ] **7. Apakah penghapusan backup dibatasi?**
  Hanya pihak tertentu yang boleh menghapus salinan atau mengubah retensi
- [ ] **8. Apakah autentikasi multifaktor telah digunakan?**
  Lindungi akun backup dan jangan pakai ulang kata sandi
- [ ] **9. Apakah restore pernah diuji?**
  File, folder, database, mesin virtual, dan aplikasi beserta konfigurasinya
- [ ] **10. Apakah waktu restore aktual sudah diketahui?**
  Bandingkan dengan batas waktu berhentinya operasional
- [ ] **11. Apakah retensi mencakup beberapa titik pemulihan?**
  Versi harian, mingguan, atau bulanan untuk serangan yang terlambat terdeteksi
- [ ] **12. Apakah SOP penanganan insiden sudah tersedia?**
  Urutan isolasi, pemilihan titik pemulihan bersih, restore, dan verifikasi
- [ ] **13. Apakah pihak yang berwenang melakukan restore sudah ditetapkan?**
  Penanggung jawab teknis, pengambil keputusan, dan pemilik sistem

*Jika satu elemen kritis belum tersedia, backup belum bisa dianggap siap dipakai saat serangan ransomware.*