

#### **Step 4. Control Analysis**

Tujuan dari langkah ini adalah untuk mendokumentasikan dan menilai efektivitas kontrol teknis dan non-teknis yang telah atau akan diterapkan oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan (atau probabilitas) dari sumber ancaman yang mengeksploitasi kerentanan sistem.

*Input* : current controls, planned controls atau kontrol saat ini, kontrol yang direncanakan .

*Output* : Daftar kontrol saat ini atau yang direncanakan (kebijakan, prosedur, pelatihan, mekanisme teknis, asuransi, dll.) yang digunakan untuk sistem TI untuk mengurangi kemungkinan kerentanan yang dilakukan dan mengurangi dampak dari peristiwa yang merugikan tersebut.

#### **Step 8. Control Recommendations**

Tujuan dari langkah ini adalah untuk mengidentifikasi kontrol yang dapat mengurangi atau menghilangkan risiko yang diidentifikasi, yang sesuai dengan operasi organisasi. Tujuan dari kontrol ini adalah untuk mengurangi tingkat risiko terhadap sistem dan data ke tingkat yang dapat diterima. Faktor-faktor yang perlu dipertimbangkan ketika mengembangkan kontrol dapat mencakup efektivitas opsi yang direkomendasikan (yaitu, kompatibilitas sistem), undang-undang dan peraturan, kebijakan organisasi, dampak operasional, serta keselamatan dan keandalan. Rekomendasi kontrol memberikan masukan untuk proses mitigasi risiko, di mana kontrol keamanan prosedural dan teknis yang direkomendasikan dievaluasi, diprioritaskan, dan diimplementasikan.

*Output* : Recommendation of controls dan solusi alternatif untuk memitigasi risiko.

#### **Step 9. Results Documentation**

Hasil penilaian risiko didokumentasikan dalam laporan atau pengarahannya resmi dan diberikan kepada manajemen senior (pemilik misi) untuk membuat keputusan tentang kebijakan, prosedur, anggaran, dan perubahan operasional dan manajemen sistem.

*Output* : Risk assessment report atau laporan penilaian risiko yang menggambarkan ancaman dan kerentanan, mengukur risiko, dan memberikan rekomendasi untuk implementasi kontrol.

