

Risk domain	Enterprise impact
Execution control loss	Agent takes actions that cannot be reversed: incorrect transactions, unauthorized communications, operational disruptions
Unauthorized tool use	Agent accesses systems or APIs outside its intended scope, creating data exposure or triggering unintended downstream effects
Privilege escalation	Agent accumulates permissions beyond its original scope over time, or inherits broad permissions from its deployment context
Data misuse	Agent accesses, processes, or shares data beyond its authorized scope, creating privacy violations and regulatory exposure
Multi-agent emergence	Combined behavior of multiple agents produces outcomes that no individual agent was designed to create