# CompTIA Security+ SY0-701 Risk Management Cheat Sheet

secplusmastery.com

Risk formulas, responses, recovery metrics, and third-party agreements. A free study resource.

*Domain 5 risk and governance in one place: the formulas, the four risk responses, the recovery metrics, recovery sites, and the third-party agreements you will be tested on.*

## Risk fundamentals and formulas

*The vocabulary and the math. Risk is the chance a threat exploits a vulnerability, weighted by impact.*

**Risk = Likelihood x Impact** The core idea: a threat exploiting a vulnerability, weighted by how likely it is and how bad it would be.

**Vulnerability / Threat / Risk** A vulnerability is a weakness, a threat is what could exploit it, and risk is the likelihood and impact if the two meet.

**EF (Exposure Factor)** The percentage of an asset's value lost in a single incident, from 0 to 100%.

**SLE (Single Loss Expectancy)** Asset Value x Exposure Factor. The cost of one occurrence.

**ARO (Annualized Rate of Occurrence)** How many times per year you expect the event to happen.

**ALE (Annualized Loss Expectancy)** SLE x ARO. The expected yearly cost of the risk.

**Inherent vs residual risk** Inherent risk is before any controls; residual risk is what remains after controls are applied.

**Risk appetite vs tolerance** Appetite is how much risk an organization is willing to take overall; tolerance is the acceptable variance around it.

## Responding to risk

*Once a risk is identified, you choose a response. Know the four classic options.*

**Accept** Take no further action because the cost of control exceeds the risk. May be formalized as an exemption or exception.

**Avoid** Stop the activity that creates the risk entirely.

**Transfer (share)** Shift the financial impact to a third party, such as insurance or outsourcing.

**Mitigate (reduce)** Apply controls to lower the likelihood or the impact.

**Risk register** The central record of each risk: owner, score, chosen response, and status.

**Risk owner** The person accountable for managing a specific risk.

## Risk analysis types

*How risks are measured and prioritized. The exam contrasts qualitative with quantitative.*

**Qualitative** Rates risk with labels such as high, medium, and low on a likelihood-impact matrix. Fast but subjective.

**Quantitative** Assigns hard numbers and money: SLE, ARO, and ALE. Rigorous but data-heavy.

**Risk matrix / heat map** Plots likelihood against impact to rank which risks to treat first.

**KRI (Key Risk Indicator)** A metric that signals rising risk before it is realized.

**Assessment cadence** Risk assessments can be ad hoc, one-time, recurring, or continuous.

## Continuity and recovery metrics

*How resilience and disaster recovery are measured. These come out of the business impact analysis.*

**BIA (Business Impact Analysis)** Identifies critical functions and the impact of their downtime, and sets the RTO and RPO.

**RTO (Recovery Time Objective)** Maximum tolerable time to restore a service after an outage. RTO = time.

**RPO (Recovery Point Objective)** Maximum tolerable data loss, measured back to the last good backup. RPO = data.

**MTD (Maximum Tolerable Downtime)** The longest a function can be down before serious harm. RTO must be shorter than MTD.

**MTBF (Mean Time Between Failures)** Average time between failures of a repairable system. Higher means more reliable.

**MTTR (Mean Time To Repair)** Average time to restore a failed system. Lower is better.

**MTTF (Mean Time To Failure)** Average lifespan of a non-repairable component.

## Recovery sites and resilience

*Where you fail over to, traded off by cost versus how fast they come up.*

**Hot site** Fully equipped and running; fail over in minutes. Most expensive.

**Warm site** Hardware and connectivity ready, but needs data and setup. Comes up in hours.

**Cold site** Space and power only; everything must be brought in. Cheapest and slowest.

**Geographic dispersion** Spread sites and backups far enough apart that one disaster cannot hit them all.

**High availability** Redundancy, clustering, and load balancing to remove single points of failure.

## Third-party agreements

*The contracts and documents that govern vendor and partner relationships, all tested in Domain 5.*

**SLA (Service Level Agreement)** Measurable commitments such as uptime, response times, and penalties.

**MOU / MOA (Memorandum of Understanding/Agreement)** A less formal statement of intent to cooperate; often not legally binding.

**MSA (Master Service Agreement)** Overarching terms that govern future work and individual statements of work.

**SOW (Statement of Work)** The specific deliverables, scope, and timeline of a project.

**BPA (Business Partners Agreement)** Terms between business partners, such as responsibilities and profit sharing.

**NDA (Non-Disclosure Agreement)** Legally binds the parties to keep shared information confidential.

**AUP (Acceptable Use Policy)** The rules for how employees may use company systems and data.

## Governance, audits, and data roles

*Who sets the rules, who checks them, and who is responsible for the data.*

**Policy / standard / procedure / guideline** Policy is high-level intent, a standard is mandatory specifics, a procedure is step-by-step, and a guideline is recommended but optional.

**Due care vs due diligence** Due care is taking reasonable action; due diligence is the ongoing investigation and monitoring that informs it.

**Separation of duties** Split a sensitive task so no single person controls it end to end.

**Internal vs external audit** Internal audits are self-checks; independent external audits and attestation carry more trust.

**Data owner vs custodian** The owner is accountable for the data and its classification; the custodian implements the controls day to day.

**Controller vs processor** Under privacy law the controller decides why and how data is processed; the processor acts on the controller's behalf.