FreeFellow

FORMULA SHEET

CPA ISC

Information Systems & Controls

10
FORMULAS

3
TOPICS

freefellow.org/cpa-isc/formulas

INFORMATION SYSTEMS AND DATA MANAGEMENT

4 items

RPO vs. RTO

RPO (Recovery Point Objective): max acceptable data loss in time (how old can restored data be?).

RTO (Recovery Time Objective): max acceptable downtime.

RPO drives backup frequency; RTO drives recovery infrastructure.

MTBF and system availability

$$\text{MTBF} = \frac{\text{Total Operational Time}}{\text{Number of Failures}}$$

$$\text{Availability} = \frac{\text{MTBF}}{\text{MTBF}+\text{MTTR}}$$

MTTR = Mean Time to Repair. Higher MTBF or lower MTTR → higher availability.

Data classification levels

Government: Top Secret → Secret → Confidential → Unclassified.

Commercial: Restricted → Confidential → Internal → Public.

Drives access controls, handling, and retention.

Backup site tiers

Cold: basic infrastructure only; lowest cost, longest RTO (days–weeks).

Warm: partial equipment; moderate cost/RTO (hours–days).

Hot: fully mirrored, real-time; highest cost, lowest RTO (minutes–hours).

SECURITY, CONFIDENTIALITY AND PRIVACY

5 items

Access control models: DAC, MAC, RBAC

DAC (Discretionary): owner sets permissions (Windows file share).

MAC (Mandatory): security labels enforce access (gov/military).

RBAC (Role-Based): perms assigned to roles; users to roles (enterprise).

Information security risk formula

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

Controls reduce vulnerability or impact. Risk = residual risk after controls applied.

Annual loss expectancy (ALE)

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

SLE = Single Loss Expectancy (loss per incident), ARO = Annualized Rate of Occurrence.

Control is cost-effective if cost of control < ALE reduction achieved.

NIST password guidelines (SP 800-63B)

Min length 8 (15 for admin).

No complexity rules.

No forced rotation unless compromise.

Screen against breached passwords.

Allow paste + password managers.

Encryption key sizes and strength

AES-128 adequate; AES-256 for sensitive.

RSA-2048 min; RSA-4096 long-term.

ECC-256 ≈ RSA-3072.

NIST: 112-bit min through 2030; 128-bit beyond.

CONSIDERATIONS FOR SOC ENGAGEMENTS

1 item

SOC report types

SOC 1: ICFR — for FS auditors.

SOC 2: Trust Services Criteria (Security, Availability, Integrity, Confidentiality, Privacy).

SOC 3: Public summary of SOC 2.

Type I = design (point in time). Type II = design + operating effectiveness (period).