COMPTIA SECURITY+ SY0-701 · WEEK 2

Security Controls and Risk Analysis Fundamentals



Objectives 1.1 and 5.2 · 90-minute workshop

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Classify controls by category and type
2. Select a control type for a stated risk
3. Calculate SLE and ALE
4. Compare qualitative and quantitative analysis
5. Recommend a treatment with a cost-benefit check
6. Distinguish risk appetite from risk tolerance
7. Define RTO, RPO, MTTR, and MTBF

AGENDA

5 min	Introduction
20 min	Controls and Exercise 1
25 min	Risk analysis and calculations
15 min	Register, appetite, treatment
5 min	Business impact analysis
15 min	Exercise 2: clinic scenario
5 min	Review and takeaways

Categories describe how a control is carried out



Technical

Implemented through systems and software.

Examples: Firewall, encryption, MFA



Managerial

Administrative controls that govern risk.

Examples: Risk assessments, security policies



Operational

Carried out by people and processes.

Examples: Awareness training, change management



Physical

Protect facilities and equipment.

Examples: Badge readers, locks, cameras

Types describe what a control does

Preventive

Stops an event

Access control list

Deterrent

Discourages an attempt

Warning banner, visible camera

Detective

Identifies an event during or after

SIEM alert, log review

Corrective

Reduces impact after an event

Restore from backup

Compensating

Substitutes for an infeasible control

Extra monitoring on a legacy system

Directive

Instructs behavior

Acceptable use policy

KEY POINT A control has one category and can serve one or more types.

EXERCISE 1 · INDIVIDUAL

Classify the control



8

MINUTES

Write a category and a type for each control. Be ready to defend your answer.

#	Control	Category	Type
1	Firewall rule blocking inbound traffic		
2	Alert on repeated failed logins		
3	Annual security awareness training		
4	Badge reader on the server room door		
5	Restoring a server from backup after ransomware		
6	“Unauthorized access prohibited” login banner		
7	Written password policy		
8	Security camera pointed at the data center entrance		
9	Extra log monitoring on an unpatchable legacy device		
10	Quarterly vulnerability scan		

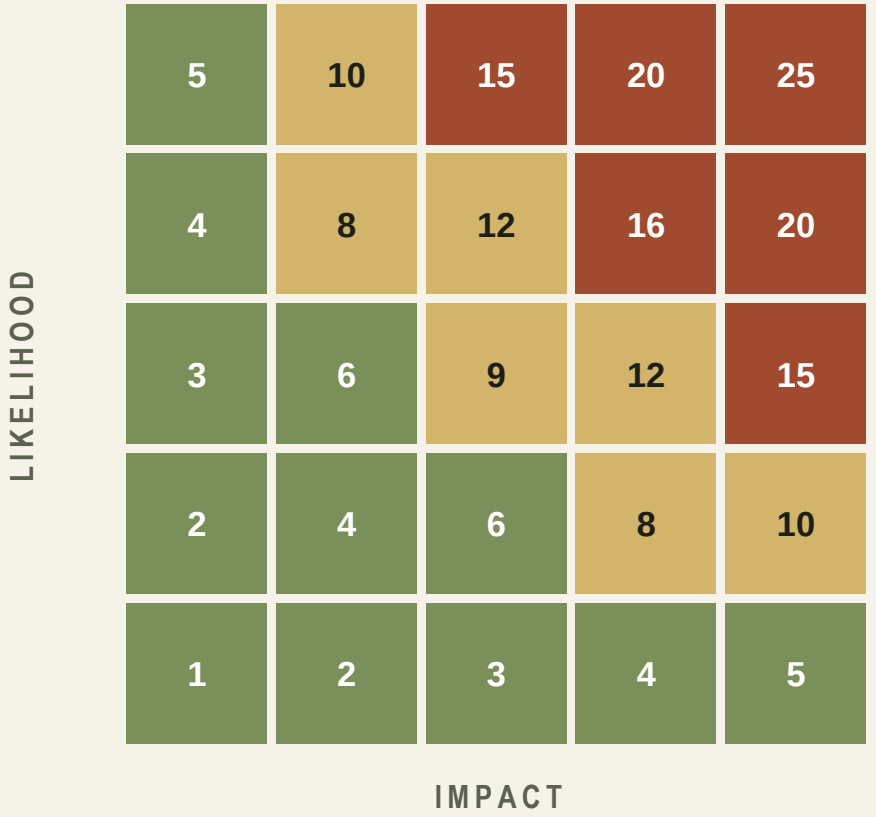
Risk is a function of likelihood and impact

Threat — Anything that can cause harm: an attacker, a flood, a careless insider.

Vulnerability — A weakness a threat can exploit: an unpatched server, an unlocked door.

Likelihood — How probable it is that the threat exploits the weakness.

Impact — How much harm results if it does.



Score = likelihood x impact, each rated 1 to 5

IDENTIFICATION

Find the assets, the threats to them, and their vulnerabilities.

ASSESSMENT TYPES

- Ad hoc
- Recurring
- One-time
- Continuous

Qualitative vs quantitative analysis

Qualitative

Ratings such as low, medium, and high. Fast and useful when data is thin, but it relies on judgment.

Low | Medium | High

Quantitative

Dollar values. Slower and needs data, but it tells you what a control is worth.

SLE = asset value x exposure factor
ALE = SLE x ARO

WORKED EXAMPLE

$200,000
Asset value

25%
Exposure factor

0.5
ARO: once in 2 years

$50,000
SLE

$25,000
ALE per year

The risk register is a living record with owners

ID	Risk	Owner	Rating	Treatment	KRI	Status
R1	Theft of unencrypted laptop with patient records	Office manager	**High**	Mitigate: disk encryption	Laptops without encryption	In progress
R2	Misuse of the shared admin account	IT lead	**Medium**	Mitigate: named accounts, MFA	Logins to shared accounts	Open



Risk owner

The person accountable for a risk and its treatment. Name a role, not a team.



Key risk indicator

An early, measurable signal that a risk is changing. Example: count of laptops without encryption.



Appetite and tolerance

Appetite is the amount and type of risk pursued. Tolerance is the acceptable variation for one risk.

APPETITE **Expansionary** more risk for growth **Neutral** balanced **Conservative** less risk, more stability

Choose a treatment, then check the cost

Mitigate

Add controls to reduce likelihood or impact

Transfer

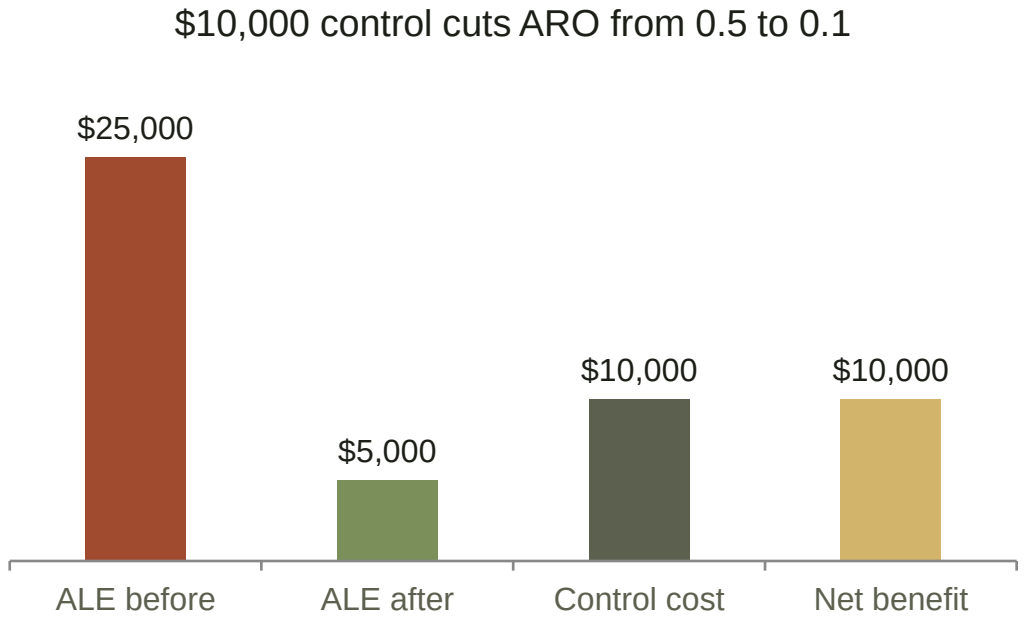
Shift the financial impact, for example insurance

Accept

Document the decision: exemption or exception

Avoid

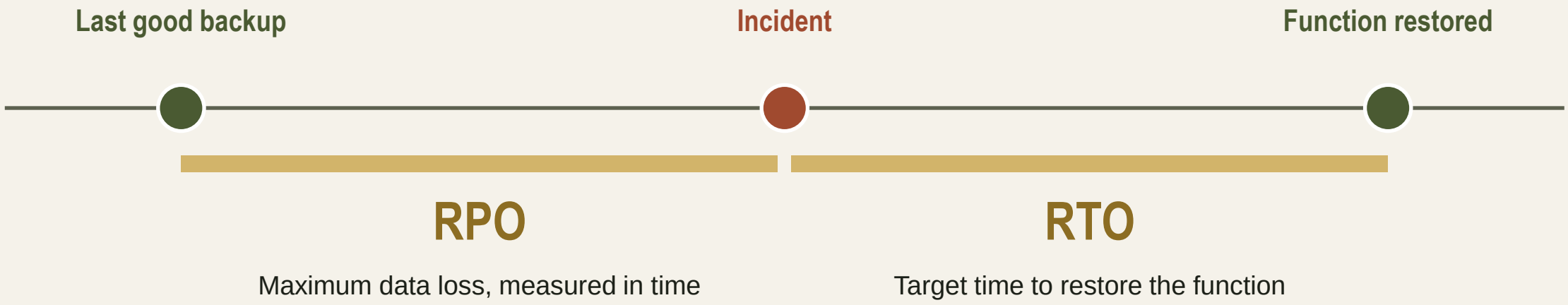
Stop the activity that creates the risk



Reduction **$20,000** minus cost **$10,000** = net **$10,000**

The control pays for itself, so mitigation is justified.

A BIA ranks functions and sets recovery targets



MTTR

Mean time to repair: how long a fix takes on average.

MTBF

Mean time between failures: how long a component runs before it fails.

EXERCISE 2 · SMALL GROUPS

Small clinic scenario

A small clinic stores patient records on laptops without disk encryption and uses a single shared admin account.

Risk A: laptop theft

$150,000	40%	0.3
Asset value	Exposure factor	ARO

Risk B: unauthorized admin access

$300,000	20%	0.2
Asset value	Exposure factor	ARO

YOUR TASKS

1. Calculate SLE and ALE for each risk.
2. Choose a treatment strategy for each.
3. Name one control for each, with its category and type.
4. Encryption costs $6,000 a year and cuts Risk A's ARO to 0.05. Is it worth it?

10 min in groups, 5 min debrief

REVIEW

Five questions: write your answers first

1. A firewall blocks inbound traffic from unknown sources. What are its category and type?
2. Asset value $120,000, exposure factor 50%, ARO 0.25. What is the ALE?
3. Management buys cyber insurance for a risk it cannot reduce further. Which strategy is this?
4. What is the difference between risk appetite and risk tolerance?
5. A restore point is set at four hours of data loss. Which BIA metric is this?

TAKEAWAYS

Four things to take with you

01

Classify controls clearly

One category, one or more types. Name both.

02

Quantify risk when you can

ALE tells you what a control is worth.

03

Tie treatment to appetite

Every decision fits the organization’s appetite and tolerance.

04

Set recovery targets with a BIA

RTO and RPO come from how critical each function is.

NEXT Lab 2: start the Lakeside Family Clinic risk register (see your handout).