STUDENT HANDOUT · WEEK 2

# Security Controls and Risk Analysis Fundamentals

Reference sheets, exercise worksheets, review questions, and Lab 2

| | |
|---|---|
| Name | |
| Date | |
| Group (Exercise 2) | |

## FORMULA REFERENCE

| Term | Formula or meaning | Example |
|---|---|---|
| SLE (single loss expectancy) | Asset value x exposure factor | $200,000 x 25% = $50,000 |
| ALE (annualized loss expectancy) | SLE x ARO | $50,000 x 0.5 = $25,000 |
| ARO (annualized rate of occurrence) | How many times a year the event is expected | 0.5 = once every two years |
| EF (exposure factor) | Share of the asset lost in one event | 25% = a quarter of the value |
| Net benefit of a control | ALE reduction minus annual control cost | $20,000 minus $10,000 = $10,000 |
| RTO (recovery time objective) | Target time to restore a function | Payroll back within 8 hours |
| RPO (recovery point objective) | Maximum acceptable data loss, measured in time | No more than 4 hours of data lost |
| MTTR (mean time to repair) | Average time to fix a failed component | Repairs take 3 hours on average |
| MTBF (mean time between failures) | Average time a component runs between failures | A drive fails every 50,000 hours on average |

# CONTROL REFERENCE

| Categories (how it is carried out) | Types (what it does) |
|---|---|
| **Technical:** systems and software. Firewall, encryption, MFA. | **Preventive:** stops an event. Access control list. |
| **Managerial:** governs risk. Risk assessments, security policies. | **Deterrent:** discourages an attempt. Warning banner. |
| **Operational:** people and processes. Awareness training, change management. | **Detective:** finds an event during or after. SIEM alert. |
| **Physical:** facilities and equipment. Badge readers, locks, cameras. | **Corrective:** reduces impact after. Restore from backup. |
| A control has **one** category. | **Compensating:** substitutes for a primary control that is not feasible. |
| It can serve **one or more** types. | **Directive:** instructs behavior. Acceptable use policy. |

# EXERCISE 1: CLASSIFY THE CONTROL

For each control, write its category and its type. Be ready to defend your answer. Some controls serve more than one type.

| # | 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 | | |

# EXERCISE 2: SMALL CLINIC SCENARIO

**SCENARIO**

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

| | Risk A: laptop theft | Risk B: unauthorized admin access |
|---|---|---|
| Asset value | $150,000 | $300,000 |
| Exposure factor | 40% | 20% |
| ARO | 0.3 | 0.2 |

**Tasks**

1. Calculate SLE and ALE for each risk.
2. Choose a treatment strategy for each risk (mitigate, transfer, accept, or avoid).
3. Name one control for each risk, with its category and type.
4. Disk encryption costs $6,000 per year and cuts the ARO for Risk A to 0.05. Is it worth it?

| | Risk A | Risk B |
|---|---|---|
| SLE | | |
| ALE | | |
| Strategy | | |
| Control (category, type) | | |

**Cost-benefit check for encryption (Risk A)**

| Step | Your work |
|---|---|
| New ALE with encryption | |
| ALE reduction | |
| Net benefit (minus $6,000) | |
| Decision | |

## REVIEW QUESTIONS

**1.** A firewall blocks inbound traffic from unknown sources. What are its category and type?

**2.** Asset value is $120,000, exposure factor is 50%, and ARO is 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?

## KEY TAKEAWAYS

- Classify controls clearly: one category, one or more types.
- Quantify risk when you have the data. ALE tells you what a control is worth.
- Tie every treatment decision to the organization’s appetite and tolerance.
- Use a business impact analysis to set recovery targets (RTO and RPO).

# LAB 2: START A RISK REGISTER

**60 MINUTES · 20 POINTS · DUE BEFORE THE NEXT CLASS**

Lakeside Family Clinic is a fictional 25-person clinic. It stores patient records on staff laptops without disk encryption, uses a single shared administrator account, keeps a file server in an unlocked supply closet, and backs up to an external drive that stays plugged in. You will use this clinic all semester.

### Steps

1. Open a spreadsheet and create the columns shown below.
2. List at least five clinic assets (for example patient records, laptops, file server, scheduling system, backups).
3. Write at least five specific risks. Name the threat, the vulnerability, and the asset in each one.
4. Rate likelihood and impact from 1 (low) to 5 (high). Score = likelihood x impact.
5. Assign an owner by role (for example office manager or lead physician), a treatment strategy, and one key risk indicator.
6. For two risks, add a quantitative SLE and ALE. State your assumptions for asset value, exposure factor, and ARO.
7. Submit the spreadsheet with one sentence per risk explaining your treatment choice.

| ID | Risk | Owner | L | I | Score | Strategy | KRI |
|---|---|---|---|---|---|---|---|
| R1 | Thief steals an unencrypted laptop holding patient records | Office manager | 3 | 5 | 15 | Mitigate | Laptops without encryption |
| R2 | | | | | | | |
| R3 | | | | | | | |

Row R1 is an example. This register becomes part of Project milestone 1, due in week 4.