KK09 — Mitigation measures to reduce or eliminate threats, vulnerabilities and risks

Cyber Security · Comprehensive exam study guide

Mitigation means reducing or removing a risk. This KK ties KK03 (vulnerabilities) and KK04 (controls) together: given a threat, propose suitable measures and justify them.

Common mitigation measures

Measure	Addresses
Multi-factor authentication (MFA) & strong IAM	Unauthorised access, weak passwords, insider misuse.
Encryption (storage & transit)	Data theft and man-in-the-middle interception.
Regular updates/patching	Known vulnerabilities in unpatched software.
Code review & secure-coding standards	Insecure code and flaws reaching production.
Separated environments & access logging	Exposure of real data; detecting misuse.
Backups & incident response plan	Recovery from malware/ransomware and breaches.
Staff training & onboarding	Human error, phishing and insider risk (links to KK10).

Choosing a measure

EXAM TIP

In a scenario, name the threat, choose a measure that directly addresses it, and explain how it reduces the risk — don’t list generic measures.

Key definitions to memorise

Mitigation	A measure that reduces or eliminates a threat, vulnerability or risk.
Multi-factor authentication (MFA)	Requiring two or more proofs of identity (e.g. password plus a code) to gain access.

Exam technique

EXAM TIP

- Match the measure to the specific threat in the question.
- Explain the mechanism: how does the measure actually reduce the risk?

COMMON MISTAKES

- Listing measures that don’t address the stated threat.
- Saying ‘add security’ without naming a specific measure.

Quick revision checklist

- I can propose suitable mitigation measures for a given threat.
- I can justify how each measure reduces the risk.

Exam practice — questions & model answers

Q1. Recommend a mitigation measure for the risk of stolen passwords granting access, and justify it.

Recommend/Justify · 2 marks

Model answer

• Multi-factor authentication (1),
• because even if a password is stolen, the attacker still lacks the second factor, blocking access (1).

Q2. A team is concerned about ransomware. Describe two mitigation measures and how each helps.

Describe · 4 marks

Model answer

• Regular backups — allow data to be restored without paying a ransom (2).
• Patching/updates and staff training — close vulnerabilities and reduce the chance staff trigger the malware (2).