KK06 — Criteria for evaluating the security of software development practices within an organisation

Cyber Security · Comprehensive exam study guide

You must be able to judge **how secure** a team's development practices are, using measurable criteria. Frame criteria as questions tied to the controls in KK04.

Example evaluation criteria

- Are robust IAM and least-privilege access enforced?
- Is sensitive data encrypted in storage and transit?
- Is code reviewed before release?
- Are updates/patches applied promptly?
- Are development, testing and production environments separated?
- Is version control used with controlled access?
- Is threat modelling performed and are staff trained in secure development?

Making criteria measurable

EXAM TIP

Good criteria can be answered with evidence: 'Are 100% of patches applied within 48 hours?' beats 'Is the software up to date?'

Key definitions to memorise

Security evaluation criteria	Specific, measurable statements used to judge how secure an organisation's development practices are.

Exam technique

EXAM TIP

• Derive criteria directly from the KK04 controls — each control becomes a criterion.
• Phrase criteria as evidence-based questions.

COMMON MISTAKES

• Writing vague criteria ('is it secure?') that can't be measured.
• Listing controls without turning them into evaluation questions.

Quick revision checklist

- ■ I can write measurable criteria to evaluate development security.
- ■ I can apply criteria to judge a described practice.

Exam practice — questions & model answers

Q1. Write three criteria for evaluating the security of a team’s development practices.

Write · 3 marks

Model answer

• Any three measurable criteria, e.g.: Is data encrypted in transit and storage? (1) Is all code peer-reviewed before release? (1) Are patches applied within a set time? (1)

Q2. Explain why security evaluation criteria should be measurable.

Explain · 2 marks

Model answer

• Measurable criteria can be judged against evidence (1),

• giving an objective, justifiable assessment rather than an opinion (1).