

KK10 — Strategies for improving the security of software development practices

Cyber Security · Comprehensive exam study guide

STUDY DESIGN — YOU MUST KNOW

- onboarding/induction practices and developer training focused on secure development
- development of risk management plans

Beyond technical controls, organisations improve security through **people and process** strategies. Know the two listed strategies and how each strengthens secure development.

The two strategies

Strategy	What it involves	Benefit
Onboarding/induction & developer training	Teaching new and existing staff secure-development practices (e.g. secure coding, handling data, recognising phishing).	Reduces human error and insider risk; builds a security culture.
Risk-management plans	Identifying risks, assessing their likelihood/impact, and planning controls and responses.	Ensures risks are handled proactively, not after a breach.

Why people & process matter

REMEMBER

Most breaches involve human error. Training and risk planning address the **people and process** side that technical controls alone can't fix.

Key definitions to memorise

Risk-management plan	A document that identifies risks, assesses their likelihood and impact, and sets out controls and responses.
Secure-development training	Educating developers in practices that build and maintain secure software.

Exam technique

EXAM TIP

- Explain HOW each strategy improves security (culture, fewer errors, proactive planning).
- Connect training to reducing insider threats and phishing success.

COMMON MISTAKES

- Listing only technical controls when asked about improvement strategies.
- Describing a risk-management plan as a one-off rather than an ongoing process.

Quick revision checklist

- I can describe the two improvement strategies and their benefits.
- I can explain why people/process strategies complement technical controls.

Exam practice — questions & model answers

Q1. Describe how developer training improves the security of software development.

Describe · 2 marks

Model answer

- Training teaches staff secure-coding and safe data-handling practices and to recognise threats like phishing (1),
- reducing human error and insider risk and building a security-aware culture (1).

Q2. Explain the purpose of a risk-management plan in secure development.

Explain · 2 marks

Model answer

- It identifies risks and assesses their likelihood and impact (1),
- then sets out controls and responses so risks are managed proactively rather than after a breach (1).