A1

CRISC Exam
Passing Principles

ISACA series

CRISC Exam Passing Principles

1. CRISC Item & QAE Item Dev Guides are your friends
2. Maintain a Risk and Security point of views
3. Apply the themes
4. Filter and simplify
5. Generalize and contextualize
6. Adopt the right attitude
7. Guess (aka. ”Lucky Luke”)

1. CRISC Item & QAE Item Dev Guides are your friends

- ISACA CRISC Item Development Guide
  - http://www.isaca.org/Certification/Write-an-Exam-Question/Documents/CRISC-Item-Development-Guide-2013.pdf
- ISACA CRISC QAE Item Development Guide
  - https://www.isaca.org/Certification/Write-an-Exam-Question/Documents/CRISC-QAE-Item-Development-Guide.pdf
- Questions style
  - Multiple choice
    - Stem + 4 options
    - Multiple plausible answers
    - Single best / correct answer

2. Maintain a Risk Management point of view

- Questions are subtle but not tricky
- Have a rationale for selecting the option that you have
  - Select a response option for reasons related to InfoSec or Risk Management: oversight vs. mere management
    - e.g., Risk controls
  - “Best” answer is the one associated with better risk management, not necessarily “better” result from some other perspective
    - e.g., ”inefficient” outcome measures vs. ”efficient” activity metric

3. Apply the themes

- Exam includes few (if any) items related to the specifics of any particular risk management framework or standard
- Seek broadest understanding of item, select answer that is most generally correct
  - Apply the principles underling a given framework, rather than framework specific details
- Small number of ideas are pervasive in the CRISC book of knowledge
  - Choose question options that are consistent with the relevant principles.
  - If choosing an answer that is inconsistent with the principles, have a good (risk management) reason why the exception holds

4. Filter and simplify

- Real world governance questions are multi-faceted and requires cross domain knowledge to answer
  - Exam questions are much simpler, the test items are less so multi-faceted
- Crucial element here is to identify the single domain from which question was drawn
  - First filter / eliminate answers not connected with identified domain
  - Then, apply general principles of that domain when finding answer

5. Generalize and contextualize

- Items sometimes do not provide enough information to determine an unequivocal ”best answer” - incomplete ”by design”
- Be willing to apply your understanding of the most likely context for the question
  - Item writers are affected by their own bias about what is ”generally true” of IT and organizations and may not feel the need to include such information in the question
  - How candidate ”fills in the blanks” indicates the candidate’s knowledge of current practice / issues

6. Adopt the right attitude

- Many test items will seem to be incredibly easy
  - Most common post mortem response is disappointment rather than confirmation
- Take the test serious - 50% of candidates fail
  - Exercise caution with items that seem overly obvious, subjective or ”irrelevant”
    - Give those items a second or third read
    - ask ”what might I be missing?”
    - know what risk management principle is applied in your answer

7. Guess (aka. ”Lucky Luke”)

- Best of 4 multiple choice test
  - No penalty for guessing / incorrect answers
  - Answer every question
    - Worst case: eliminate those answers that are clearly wrong and then guess ”intelligently”; e.g. pick the option that seems to have most general applicability
  - If simply have ”no idea”
    - Select the longest response option
    - Or, ”option C” ☺