The following correction applies to page 181 of the *CISM® Review Questions, Answers & Explanations Manual 9th Edition*. The correction is boxed.

S2-251 An organization is considering a reciprocal arrangement with a similar organization as a recovery option. Which of the following is the **GREATEST** risk associated with a reciprocal arrangement?

A. Variations between the risk and impact assessments
B. Frequency of testing of the recovery and continuity plans
C. Dissimilarities in infrastructure and capacity
D. Differences in security policies and procedures

C is the correct answer.

Justification:
A. Analyses are predictive, so differences between the organizations will not affect adequacy in the event of recovery.
B. Organizations must collaborate on frequency of testing to ensure that each meets its needs. However, such agreements are generally established when arranging reciprocity and do not constitute ongoing risk.
C. If organizations have dissimilar infrastructure or lack capacity, it may be difficult to implement recovery.
D. Differences in security policies and procedures are generally addressed when establishing reciprocity and can be managed over time through monitoring and reporting.

S2-252 Which of the following is the **MOST** supportable basis for prioritizing risk for treatment?

A. Cost and asset value
B. Frequency and impact
C. Frequency and scope
D. Cost and effort

B is the correct answer.

Justification:
A. Cost to remediate is a major factor only relative to the value of the assets to which remediation applies (i.e., is remediation appropriate for this asset versus another risk treatment option?). It is ineffective as a means of prioritization across different assets, because it does not take into account their business value.
B. The balance between impact and frequency captures the adjusted probability of loss to the organization associated with each risk. Therefore, this provides an immediate and relevant basis for prioritization of treatment, with risks that are high-impact and high-frequency ranking the highest on the list.
C. Breadth of scope is not necessarily equivalent to impact. Prioritizing a risk that affects a broad range of relatively unimportant systems over a risk that impacts a single critical system would not be beneficial to the organization.
D. Effort is a subset of overall cost representing time and expertise. Unto itself, cost is not a suitable basis for prioritization.