The following correction applies to page 66 of the *CISM Review Questions, Answers & Explanations Manual 2014*. The text in the box below has been replaced.

S2-58 Which of the following is the **BEST** basis for determining the criticality and sensitivity of information assets?

A. A threat assessment
B. A vulnerability assessment
C. A resource dependency assessment
D. An impact assessment

D The criticality and sensitivity of information assets depends on the impact of the likelihood of the threats exploiting vulnerabilities in the asset and takes into consideration the value of the assets and the impairment of the value. Threat assessment lists only the threats that the information asset is exposed to; it does not consider the value of the asset and impact of the threat on the value. Vulnerability assessment lists only the vulnerabilities inherent in the information asset that can attract threats. It does not consider the value of the asset and the impact of perceived threats on the value. Resource dependency assessments provide process needs, but not impact.

S2-59 Which program element should be implemented **FIRST** in asset classification and control?

A. Risk assessment
B. Classification
C. Valuation
D. Risk mitigation

C Valuation is performed first to identify and understand the assets needing protection. Risk assessment is performed to identify and quantify threats to information assets that are selected by the first step, valuation. Classification and risk mitigation are steps following valuation.

S2-60 Which of the following is the **MOST** important consideration when performing a risk assessment?

A. Management supports risk mitigation efforts.
B. Annual loss expectations (ALEs) have been calculated for critical assets.
C. Assets have been identified and appropriately valued.
D. Attack motives, means and opportunities are understood.

C Identification and valuation of assets provides the basis for risk management efforts as it relates to the criticality and sensitivity of assets. Management support is always important, but is not relevant when determining the proportionality of risk management efforts. The annual loss expectancy (ALE) calculations are only valid if assets have first been identified and properly valued. Motives, means and opportunities should already be factored in as a part of a risk assessment.

S2-61 Why is asset classification important to a successful information security program?

A. It determines the priority and extent of risk mitigation efforts.
B. It determines the amount of insurance needed in case of loss.
C. It determines the appropriate level of protection to the asset.
D. It determines how protection levels compare to peer organizations.

C Classification is based on the value of the asset to the organization and helps establish the protection level in proportion to the value of the asset. Classification does not determine the priority and extent of the risk mitigation efforts; prioritization of risk mitigation efforts is generally based on risk analysis or a business impact analysis (BIA). Classification does not establish the amount of insurance needed; insurance is often not a viable option. Classification schemes differ from organization to organization and are often not suitable for benchmarking.