Latest Version: 6.0

Question: 1

How many steps are defined in the RMF process?
Response:

A. Three
B. Four
C. Six
D. Five

Answer: C

Question: 2

Which of the following control families belongs to the management class of security controls?
Response:

A. Media protection
B. Risk assessment
C. Access control
D. Configuration management

Answer: B

Question: 3

Why is security control volatility an important consideration in the development of a security control monitoring strategy?
Response:

A. It establishes priority for security control monitoring.
B. It indicates a need for compensating controls.
C. It identifies needed security control monitoring exceptions.
D. It provides justification for revisions to the configuration management and control plan.

Answer: A

Question: 4

Which organizational official is responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system?
Response:

A. Chief information officer (CIO)
B. Information system security engineer (ISSE)
C. Information security architect
D. Information system owner (ISO)

Answer: D

Question: 5

According to the Risk Management Framework (RMF), which role has a primary responsibility to report the security status of the information system to the authorizing official (AO) and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy?
Response:

A. Common control provider
B. Information system security officer (ISSO)
C. Independent assessor
D. Senior information assurance officer (SIAO)

Answer: A

Question: 6

Why would the authorization decision issue a determination of Not Authorized?
Response:

A. If the system is mission critical and requires an interim authority to operate.
B. If the system is not authorized (NA) to process classified information.
C. The information system is always accredited without any restrictions or limitations on its operation.
D. If it is deemed that the agency level risk is unacceptably high.

Answer: D

Question: 7

An effective security control monitoring strategy for an information system includes
Response:

A. the annual assessment of all security controls in the information system.
B. monitoring the security controls of interconnecting information systems outside the authorization boundary.
C. all controls listed in NIST SP 800-53, Revision 3.
D. active involvement by authorizing officials in the ongoing management of information system-related security risks.

Answer: D

Question: 8

System authorization programs are marked by frequent failure due to, among other things, poor planning, poor systems inventory, failure to fix responsibility at the system level, and
Response:

A. inability to work with remote teams.
B. lack of management support.
C. lack of a program management office.
D. insufficient system rights.

Answer: B

Question: 9

Which of the following relations correctly describes residual risk?
Response:

A. Residual Risk = Threats x Exploit x Asset Value x Control Gap
B. Residual Risk = Threats x Exploit x Asset Value x Control Gap
C. Residual Risk = Threats x Vulnerability x Asset Gap x Control Gap
D. Residual Risk = Threats x Vulnerability x Asset Value x Control Gap

Answer: D

Question: 10

Which National Institute of Standards and Technology Special Publication (NIST SP) 800 series document is concerned with continuous monitoring for federal information systems and organizations?

Response:

A. SP 800-144
B. SP 800-64
C. SP 800-137
D. SP 800-26

Answer: C