Question: 1

What are the four tiers of integration within the NIST Cybersecurity Framework?

A. Selective, Repeatable, Partial, and Adaptive
B. Partial, Risk Informed, Repeatable, and Adaptive
C. Corrective, Risk Informed, Repeatable. and Adaptive
D. Risk Informed, Selective, Repeatable, and Partial

Answer: B

Reference:
https://www.nist.gov/cyberframework/online-learning/components-framework

Question: 2

What procedure is designed to enable security personnel to detect, analyze, contain, eradicate, respond, and recover from malicious computer incidents such as a denial-of-service attack?

A. Disaster Recovery Plan
B. Emergency Analysis Plan
C. Crisis Communication Plan
D. Incident Response Plan

Answer: D

Reference:
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Question: 3

What determines the technical controls used to restrict access to USB devices and help prevent their Use within a company?

A. Block use of the USB devices for all employees
B. Written security policy prohibiting the use of the USB devices
C. Acceptable use policy in the employee HR on-boarding training
D. Detect use of the USB devices and report users

Answer: A

Question: 4

Concerning a risk management strategy, what should the executive level be responsible for communicating?

A. Risk mitigation
B. Risk profile
C. Risk tolerance
D. Asset risk

Answer: B

Question: 5

What process is used to identify an organization's physical, digital, and human resource, as required in their Business Impact Analysis?

A. Risk Management Strategy
B. Risk Assessment
C. Risk Treatment
D. Asset Inventory

Answer: D

Question: 6

What supports an organization in making risk management decisions to address their security posture in real time?

A. Baseline reporting
B. Continuous monitoring
C. User access reviews
D. Video surveillance

Answer: A