PK0-005^{Q&As}

PK0-005^Q&As

CompTIA Project+

Pass CompTIA PK0-005 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/pk0-005.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

A meeting agenda included the following items:

Review the goals of the project.

Review the progress of the project.

Discuss if the project is ready to move forward.

Which of the following best describes this type of meeting?

A. Stand-up

B. Monthly status

C. Gap analysis

D. Gate review

Correct Answer: D

Explanation: A gate review is a type of meeting that evaluates the completion and quality of a project stage and decides whether the project can proceed to the next stage. A gate review is a formal governance step that involves reviewing the goals, progress, risks, deliverables, and benefits of the project, and discussing if the project is still aligned with the business strategy and stakeholder expectations. A gate review can have different outcomes, such as go, kill, hold, recycle, or conditional go, depending on the assessment of the project status and viability123. References = CompTIA Project+ Study Guide: Exam PK0-005, 3rd Edition, Chapter 9: Project Change Management, p. 323; Everything Project Managers Need To Know About Gate Reviews | monday.com Blog; Gate reviews: What to do and why you need them - Rebel\\'s Guide to Project Management; Gates and How to Operate Them - GenSight

QUESTION 2

An organization was fined due to an audit finding that revealed a third-party vendor was able to see secured project information in a recently implemented system. Which of the following was the cause of this situation?

A. The ticket system provided access by default without any approval.

B. The project manager did not perform proper project planning.

C. The system is lacking proper access controls.

D. Sensitive data was incorrectly classified during the audit process.

Correct Answer: C

Explanation: The system is lacking proper access controls if a third-party vendor was able to see secured project information in a recently implemented system that resulted in a fine for the organization. Access controls are security mechanisms that regulate who or what can view, use, or modify data or resources in a system or network. Access controls typically involve authentication and authorization processes that verify the identity and permissions of users or devices before granting them access. Access controls can help to protect data confidentiality, integrity, and availability and prevent unauthorized access, misuse, or theft12

QUESTION 3

Government projects require that personnel submit to background screenings for certain clearance requirements. Which of the following best describes this process?

A. Data security

B. Operational security

C. Physical security

D. Digital security

Correct Answer: B

Explanation: Operational security is the process of identifying, protecting, and controlling sensitive information and activities from unauthorized access or disclosure. Operational security includes background screenings for personnel who need to access classified or restricted information or resources, as well as implementing policies and procedures to prevent leaks, breaches, or espionage. Operational security is essential for government projects that involve national security, defense, intelligence, or law enforcement. Operational security is different from data security, which is the process of safeguarding data from unauthorized access, use, modification, or destruction. Data security includes encryption, authentication, authorization, backup, and recovery of data. Operational security is also different from physical security, which is the process of securing physical assets, such as equipment, data, or personnel, from unauthorized access or damage. Physical security includes locks, alarms, cameras, guards, and fences. Operational security is also different from digital security, which is the process of protecting digital devices, networks, and systems from cyberattacks, malware, or hacking. Digital security includes firewalls, antivirus, VPN, and passwords. References = CompTIA Project+ Study Guide: Exam PK0-005, 3rd Edition, Chapter 9: Security Management1; CompTIA Project+ Certification Study Guide, 3rd Edition, Chapter 9: Security Management2; What is Operational Security (OPSEC)?3

QUESTION 4

During the testing phase of a project, the legal department rejected a deliverable due to compliance issues. The project manager reviewed the risk register and triggered the mitigation plan for this item. Which of the following documents should the project manager update next?

A. Schedule

B. Status report

C. Issue log

D. Task board

Correct Answer: C

Explanation: An issue log is a document that records and tracks any issues that arise during a project and how they are resolved1. It is different from a risk register, which records and tracks potential risks that may or may not occur during a project2. When a risk becomes an issue, it means that it has occurred and has a negative impact on the project. Therefore, the project manager should update the issue log next to document the compliance issue, its cause, its impact, its priority, its owner, and its resolution status3. Updating the issue log will help the project manager communicate the issue to the stakeholders, monitor the progress of the mitigation plan, and prevent similar issues from happening again4. References = CompTIA Project+ PK0-005 Certification Study Guide, Chapter 11: Executing Projects Part 2, page 331; Project Risk Mitigation Guide + Starter Kit | Smartsheet, Risk Register section; How to Make a Risk

Management Plan (Template Included) - ProjectManager, Risk Register section; Issue Log - Project Management Knowledge, Introduction section; Issue Log Template: Free Download | ProjectManager, Introduction and How to Use an Issue Log sections.

QUESTION 5

Someone claiming to be from a tax agency sent an email to a team member asking for access to the project repository. Which of the following BEST describes this scenario?

A. Social engineering

B. Phishing

C. Spoofing

D. Hacking

Correct Answer: B

Explanation: Phishing is a scenario where someone claiming to be from a legitimate organization sends an email or other message to a target person asking for sensitive information or access to a system or account. Phishing is a type of cyberattack that aims to trick the target into revealing personal or financial data or installing malware on their device. Phishing can compromise the security and privacy of the target and expose them to identity theft, fraud, or other malicious activities.