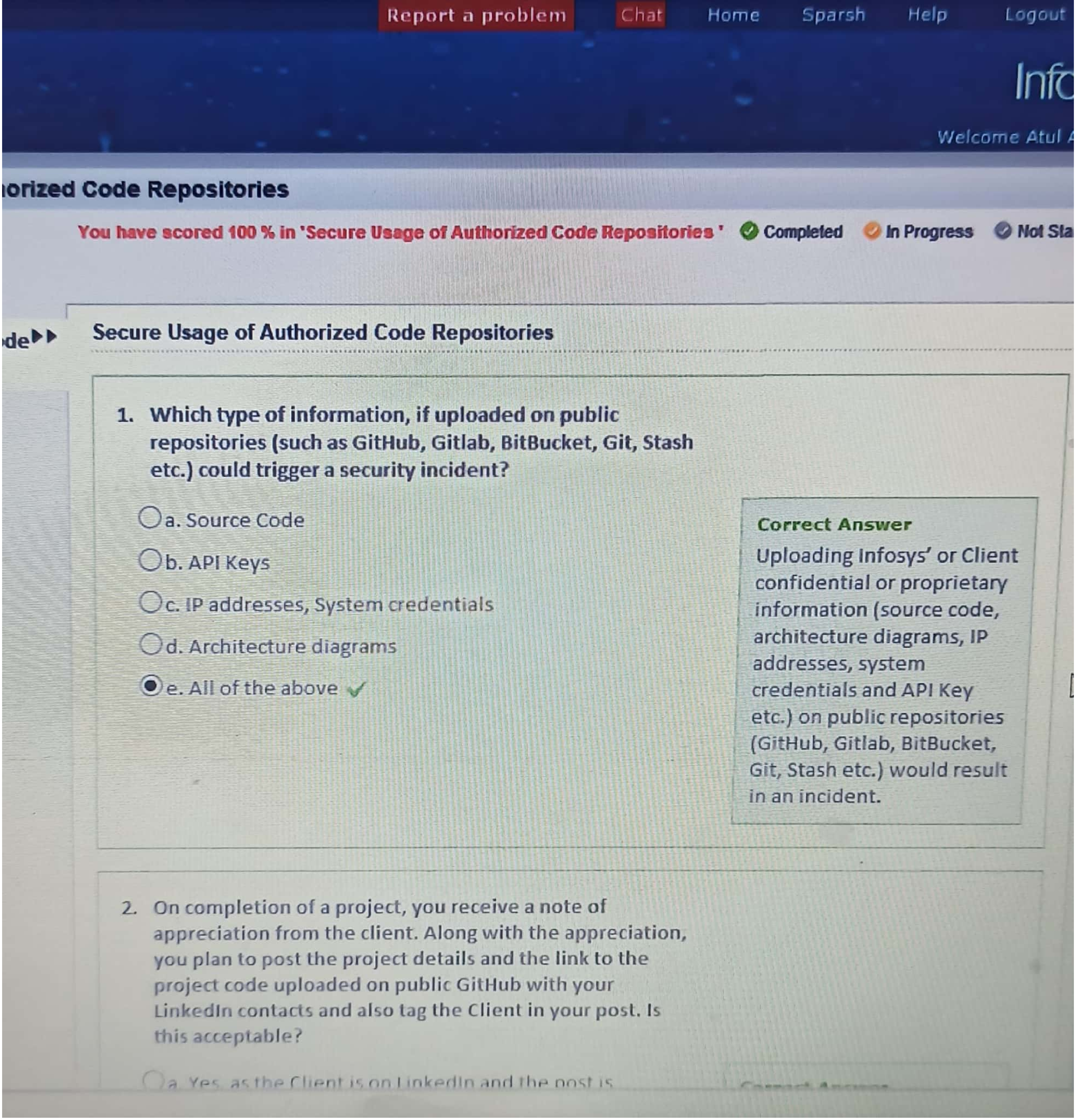


orized Code Repositories

You have scored 100 % in 'Secure Usage of Authorized Code Repositories ' ✓ Completed ● In Progress ● Not Sta

de▸▸

Secure Usage of Authorized Code Repositories

1. **Which type of information, if uploaded on public repositories (such as GitHub, Gitlab, BitBucket, Git, Stash etc.) could trigger a security incident?**

○ a. Source Code

○ b. API Keys

○ c. IP addresses, System credentials

○ d. Architecture diagrams

● e. All of the above ✓

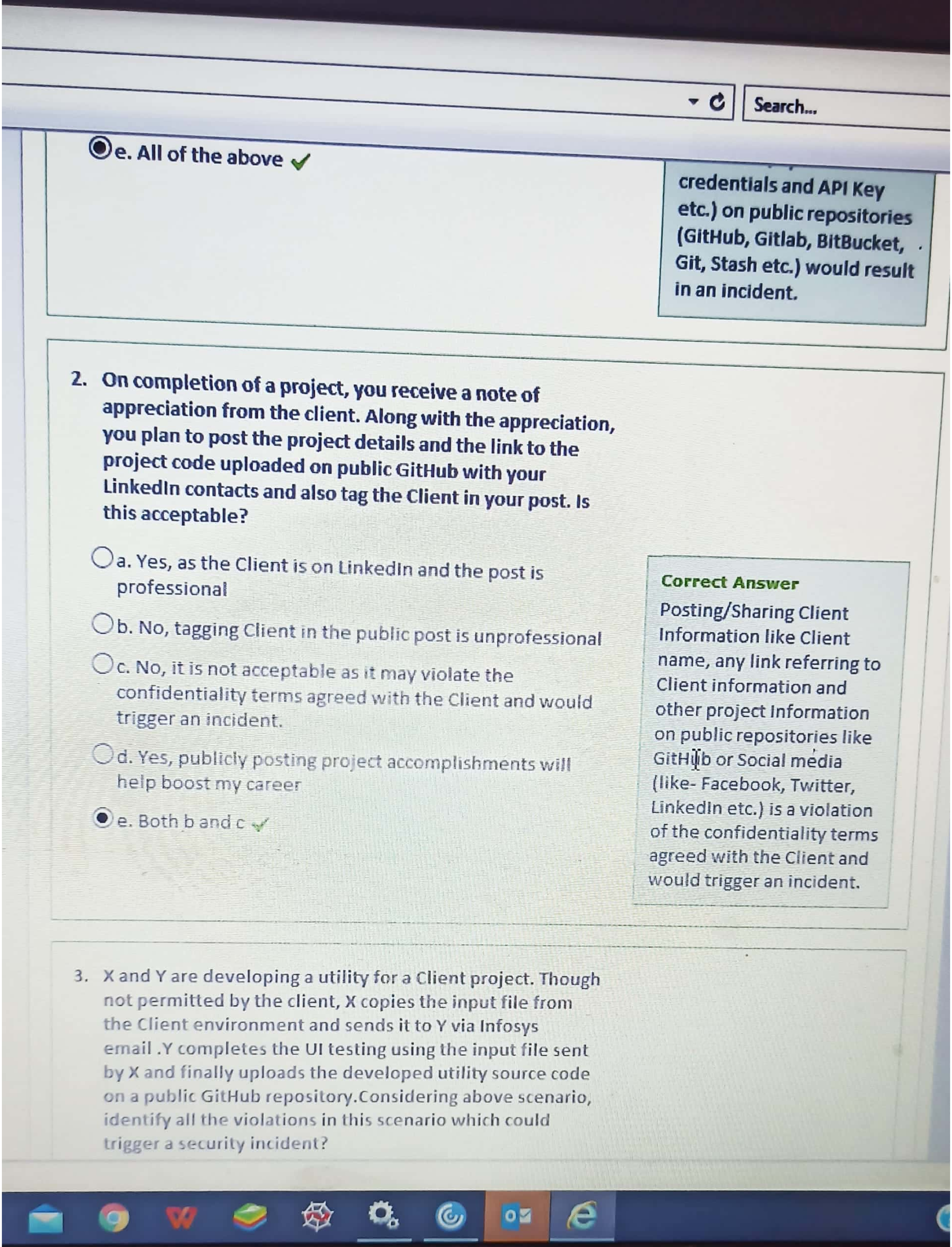
Correct Answer

Uploading Infosys' or Client confidential or proprietary information (source code, architecture diagrams, IP addresses, system credentials and API Key etc.) on public repositories (GitHub, Gitlab, BitBucket, Git, Stash etc.) would result in an incident.

2. On completion of a project, you receive a note of appreciation from the client. Along with the appreciation, you plan to post the project details and the link to the project code uploaded on public GitHub with your LinkedIn contacts and also tag the Client in your post. Is this acceptable?

○ a. Yes, as the Client is on LinkedIn and the post is

Correct Answer



● e. All of the above ✓

credentials and API Key etc.) on public repositories (GitHub, Gitlab, BitBucket, Git, Stash etc.) would result in an incident.

2. On completion of a project, you receive a note of appreciation from the client. Along with the appreciation, you plan to post the project details and the link to the project code uploaded on public GitHub with your LinkedIn contacts and also tag the Client in your post. Is this acceptable?

○ a. Yes, as the Client is on LinkedIn and the post is professional

○ b. No, tagging Client in the public post is unprofessional

○ c. No, it is not acceptable as it may violate the confidentiality terms agreed with the Client and would trigger an incident.

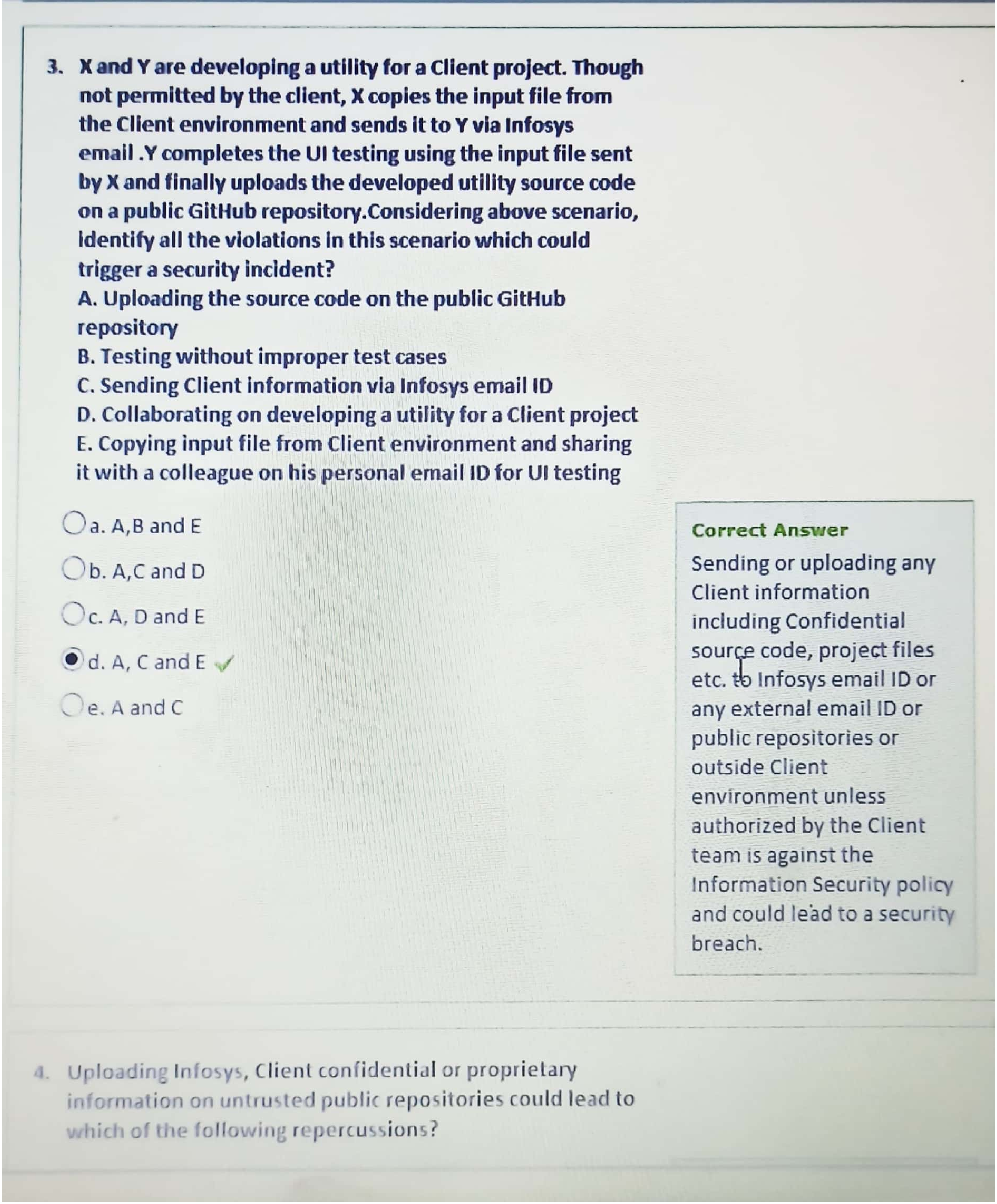
○ d. Yes, publicly posting project accomplishments will help boost my career

● e. Both b and c ✓

Correct Answer

Posting/Sharing Client Information like Client name, any link referring to Client information and other project Information on public repositories like GitHub or Social media (like- Facebook, Twitter, LinkedIn etc.) is a violation of the confidentiality terms agreed with the Client and would trigger an incident.

3. X and Y are developing a utility for a Client project. Though not permitted by the client, X copies the input file from the Client environment and sends it to Y via Infosys email .Y completes the UI testing using the input file sent by X and finally uploads the developed utility source code on a public GitHub repository.Considering above scenario, identify all the violations in this scenario which could trigger a security incident?



3. **X and Y are developing a utility for a Client project. Though not permitted by the client, X copies the input file from the Client environment and sends it to Y via Infosys email .Y completes the UI testing using the input file sent by X and finally uploads the developed utility source code on a public GitHub repository.Considering above scenario, identify all the violations in this scenario which could trigger a security incident?**
   A. Uploading the source code on the public GitHub repository
   B. Testing without improper test cases
   C. Sending Client information via Infosys email ID
   D. Collaborating on developing a utility for a Client project
   E. Copying input file from Client environment and sharing it with a colleague on his personal email ID for UI testing

○ a. A,B and E

○ b. A,C and D

○ c. A, D and E

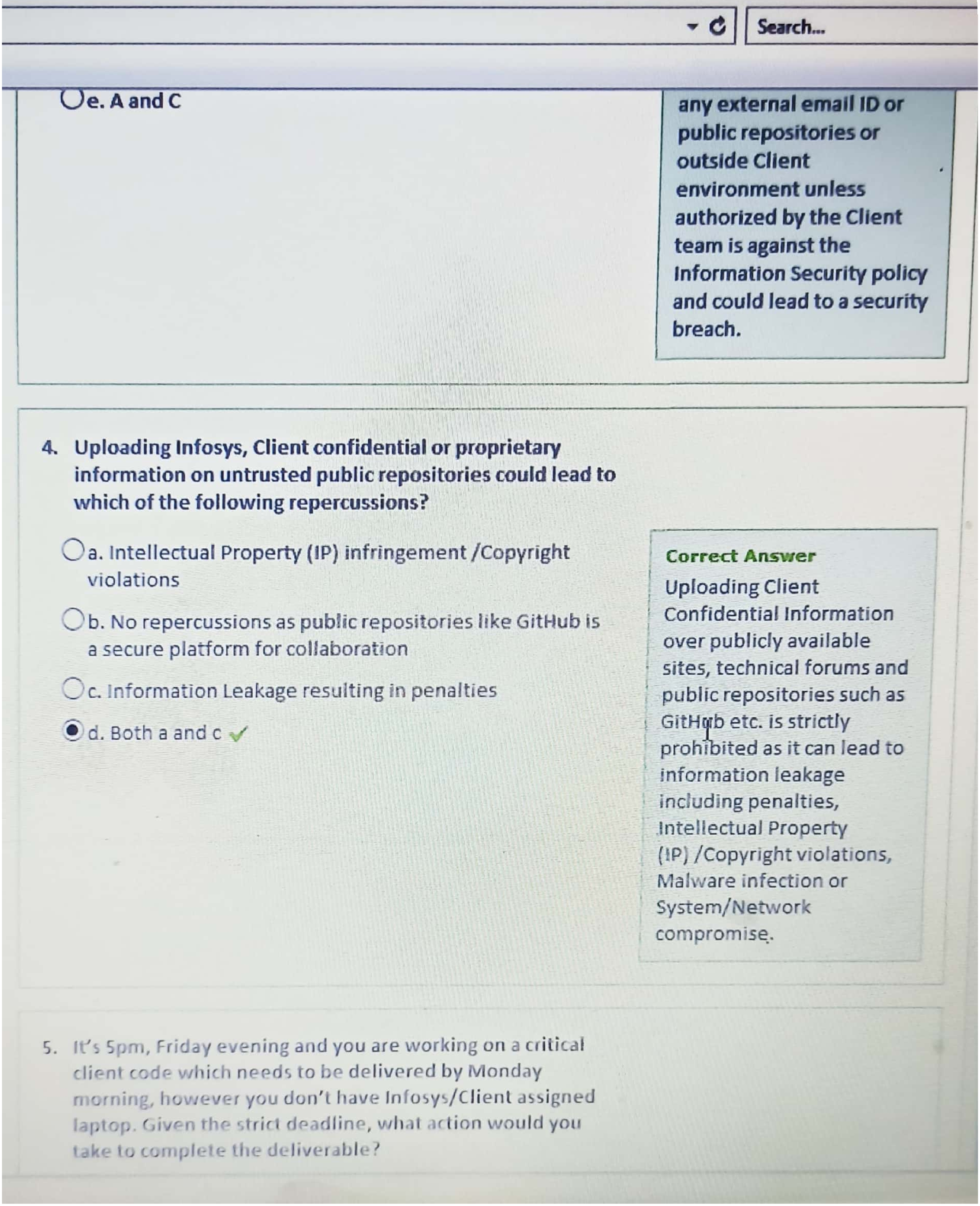
● d. A, C and E ✓

○ e. A and C

Correct Answer

Sending or uploading any Client information including Confidential source code, project files etc. to Infosys email ID or any external email ID or public repositories or outside Client environment unless authorized by the Client team is against the Information Security policy and could lead to a security breach.

4. Uploading Infosys, Client confidential or proprietary information on untrusted public repositories could lead to which of the following repercussions?



○ e. A and C

any external email ID or public repositories or outside Client environment unless authorized by the Client team is against the Information Security policy and could lead to a security breach.

4. **Uploading Infosys, Client confidential or proprietary information on untrusted public repositories could lead to which of the following repercussions?**

○ a. Intellectual Property (IP) infringement /Copyright violations

○ b. No repercussions as public repositories like GitHub is a secure platform for collaboration

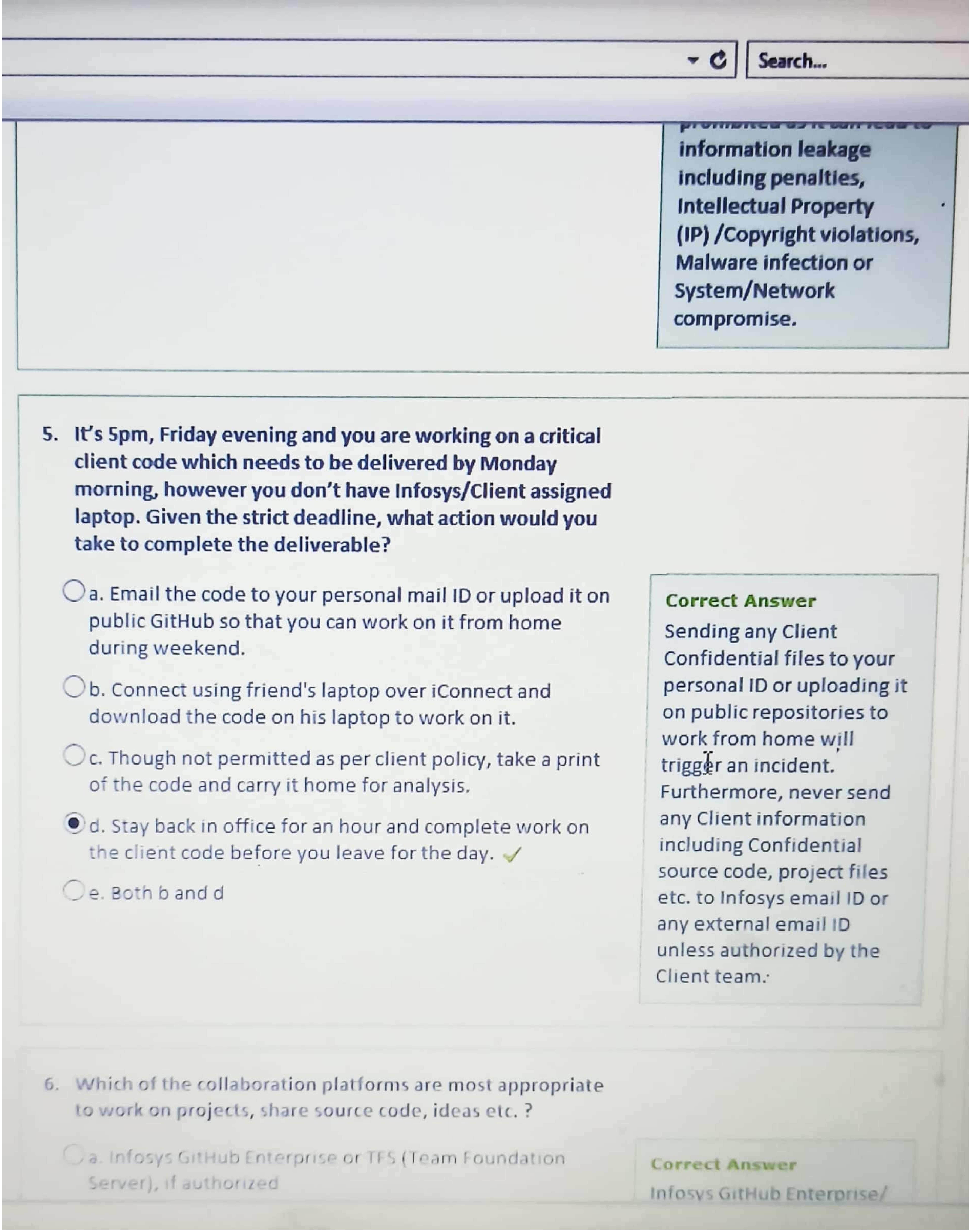
○ c. Information Leakage resulting in penalties

● d. Both a and c ✓

Correct Answer

Uploading Client Confidential Information over publicly available sites, technical forums and public repositories such as GitHub etc. is strictly prohibited as it can lead to information leakage including penalties, Intellectual Property (IP) /Copyright violations, Malware infection or System/Network compromise.

5. It's 5pm, Friday evening and you are working on a critical client code which needs to be delivered by Monday morning, however you don't have Infosys/Client assigned laptop. Given the strict deadline, what action would you take to complete the deliverable?



prohibited as it can lead to information leakage including penalties, Intellectual Property (IP) /Copyright violations, Malware infection or System/Network compromise.

5. It's 5pm, Friday evening and you are working on a critical client code which needs to be delivered by Monday morning, however you don't have Infosys/Client assigned laptop. Given the strict deadline, what action would you take to complete the deliverable?

○ a. Email the code to your personal mail ID or upload it on public GitHub so that you can work on it from home during weekend.

○ b. Connect using friend's laptop over iConnect and download the code on his laptop to work on it.

○ c. Though not permitted as per client policy, take a print of the code and carry it home for analysis.

● d. Stay back in office for an hour and complete work on the client code before you leave for the day. ✓

○ e. Both b and d

Correct Answer

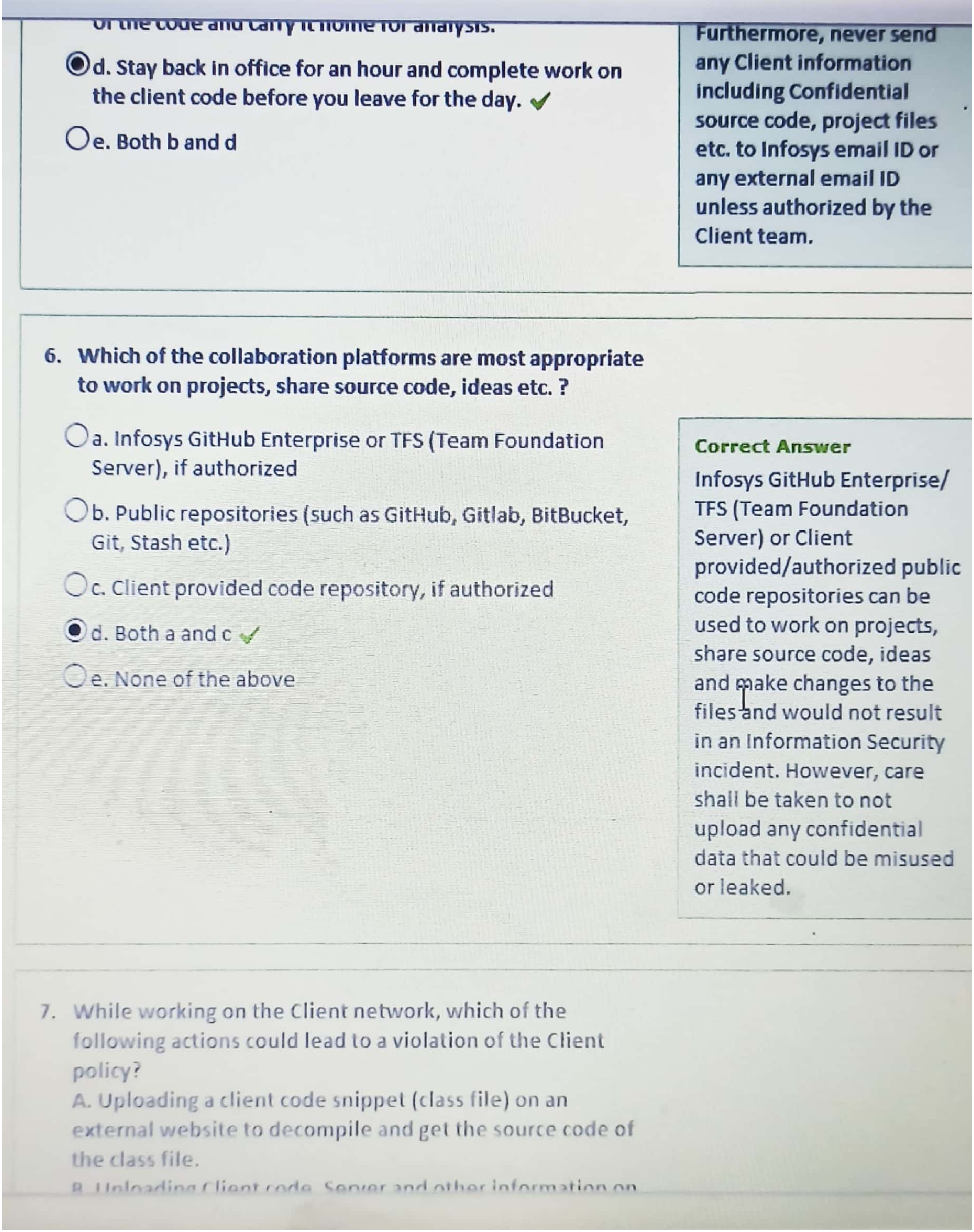
Sending any Client Confidential files to your personal ID or uploading it on public repositories to work from home will trigger an incident. Furthermore, never send any Client information including Confidential source code, project files etc. to Infosys email ID or any external email ID unless authorized by the Client team.

6. Which of the collaboration platforms are most appropriate to work on projects, share source code, ideas etc. ?

○ a. Infosys GitHub Enterprise or TFS (Team Foundation Server), if authorized

Correct Answer

Infosys GitHub Enterprise/



of the code and carry it home for analysis.

● d. Stay back in office for an hour and complete work on the client code before you leave for the day. ✓

○ e. Both b and d

Furthermore, never send any Client information including Confidential source code, project files etc. to Infosys email ID or any external email ID unless authorized by the Client team.

6. **Which of the collaboration platforms are most appropriate to work on projects, share source code, ideas etc. ?**

○ a. Infosys GitHub Enterprise or TFS (Team Foundation Server), if authorized

○ b. Public repositories (such as GitHub, Gitlab, BitBucket, Git, Stash etc.)

○ c. Client provided code repository, if authorized

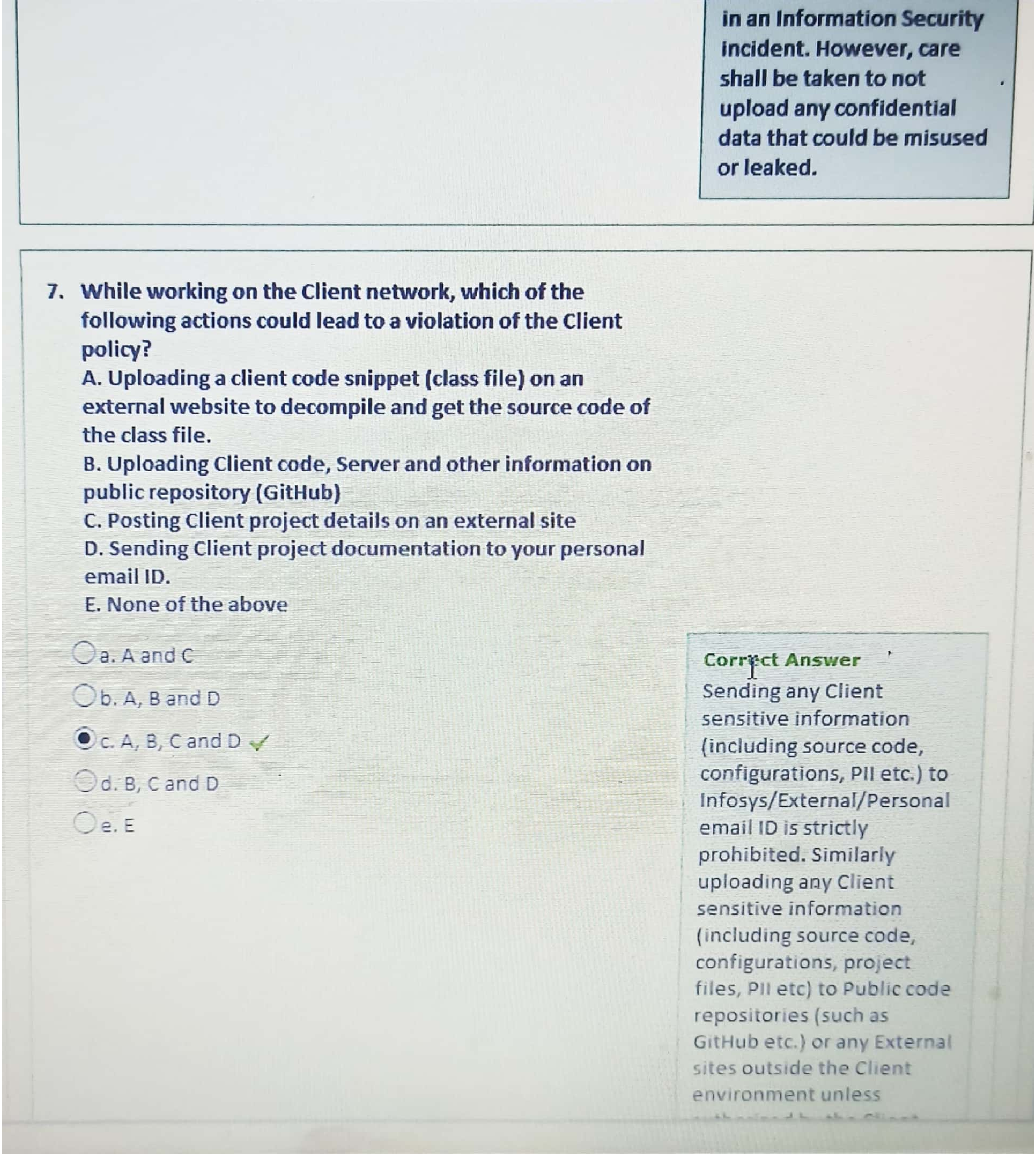
● d. Both a and c ✓

○ e. None of the above

Correct Answer

Infosys GitHub Enterprise/ TFS (Team Foundation Server) or Client provided/authorized public code repositories can be used to work on projects, share source code, ideas and make changes to the files and would not result in an Information Security incident. However, care shall be taken to not upload any confidential data that could be misused or leaked.

7. While working on the Client network, which of the following actions could lead to a violation of the Client policy?
A. Uploading a client code snippet (class file) on an external website to decompile and get the source code of the class file.
B. Uploading Client code, Server and other information on



in an Information Security incident. However, care shall be taken to not upload any confidential data that could be misused or leaked.

7. While working on the Client network, which of the following actions could lead to a violation of the Client policy?
A. Uploading a client code snippet (class file) on an external website to decompile and get the source code of the class file.
B. Uploading Client code, Server and other information on public repository (GitHub)
C. Posting Client project details on an external site
D. Sending Client project documentation to your personal email ID.
E. None of the above

○ a. A and C

○ b. A, B and D

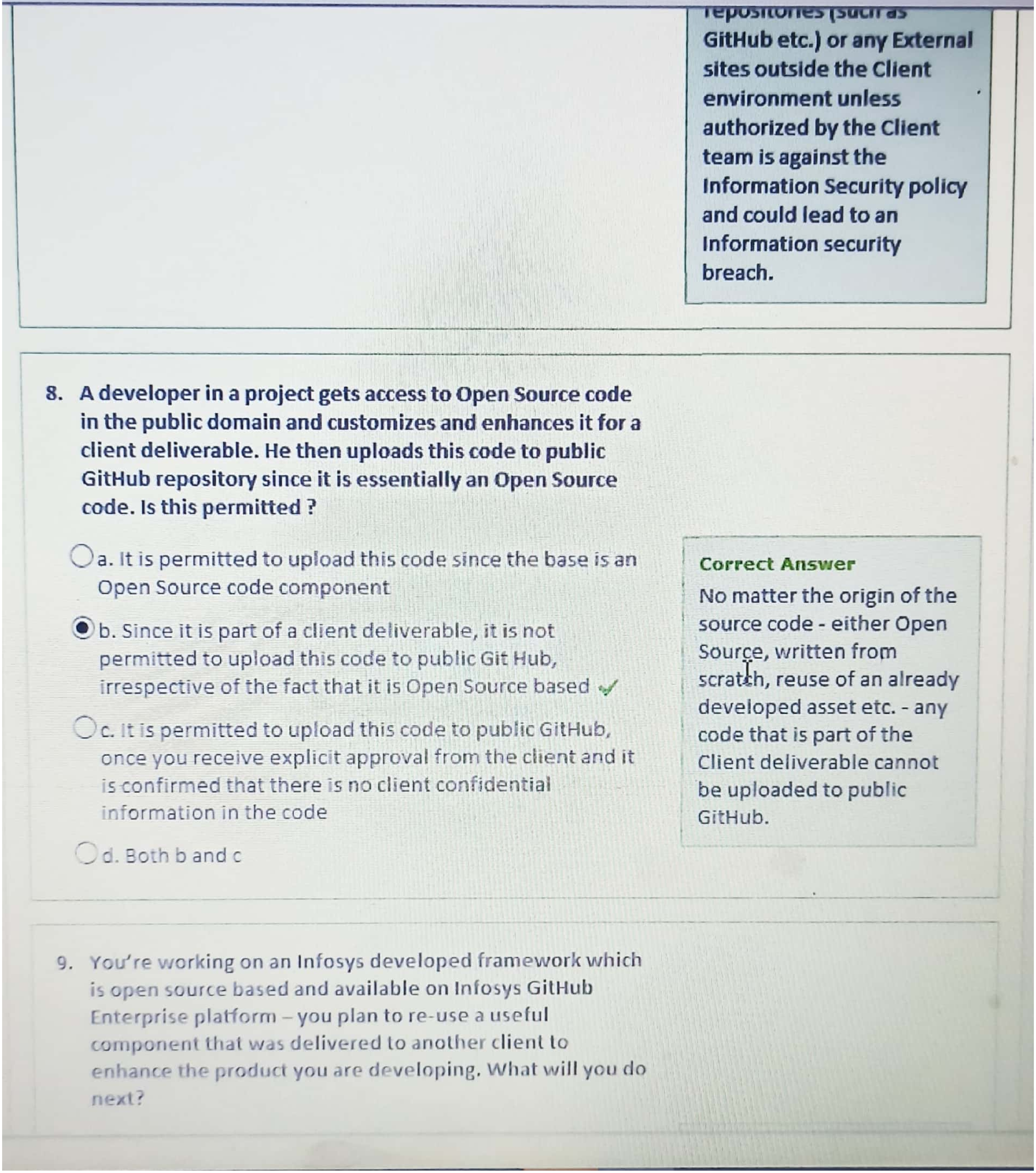
● c. A, B, C and D ✓

○ d. B, C and D

○ e. E

Correct Answer

Sending any Client sensitive information (including source code, configurations, PII etc.) to Infosys/External/Personal email ID is strictly prohibited. Similarly uploading any Client sensitive information (including source code, configurations, project files, PII etc) to Public code repositories (such as GitHub etc.) or any External sites outside the Client environment unless



repositories (such as GitHub etc.) or any External sites outside the Client environment unless authorized by the Client team is against the Information Security policy and could lead to an Information security breach.

8. A developer in a project gets access to Open Source code in the public domain and customizes and enhances it for a client deliverable. He then uploads this code to public GitHub repository since it is essentially an Open Source code. Is this permitted ?

○ a. It is permitted to upload this code since the base is an Open Source code component

● b. Since it is part of a client deliverable, it is not permitted to upload this code to public Git Hub, irrespective of the fact that it is Open Source based ✓

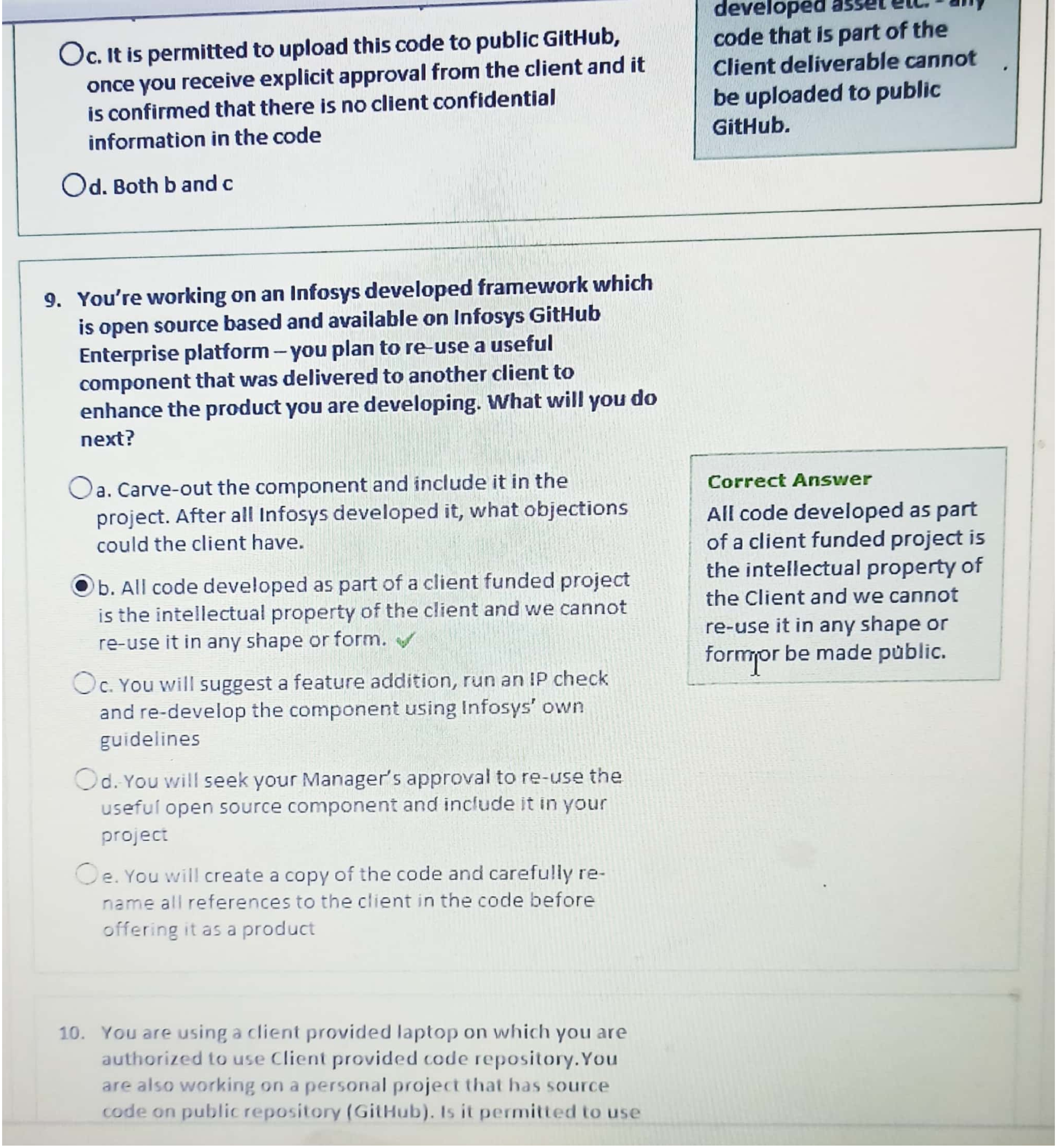
○ c. It is permitted to upload this code to public GitHub, once you receive explicit approval from the client and it is confirmed that there is no client confidential information in the code

○ d. Both b and c

Correct Answer

No matter the origin of the source code - either Open Source, written from scratch, reuse of an already developed asset etc. - any code that is part of the Client deliverable cannot be uploaded to public GitHub.

9. You're working on an Infosys developed framework which is open source based and available on Infosys GitHub Enterprise platform – you plan to re-use a useful component that was delivered to another client to enhance the product you are developing. What will you do next?



○ c. It is permitted to upload this code to public GitHub, once you receive explicit approval from the client and it is confirmed that there is no client confidential information in the code

○ d. Both b and c

developed asset etc. - any code that is part of the Client deliverable cannot be uploaded to public GitHub.

9. You're working on an Infosys developed framework which is open source based and available on Infosys GitHub Enterprise platform – you plan to re-use a useful component that was delivered to another client to enhance the product you are developing. What will you do next?

○ a. Carve-out the component and include it in the project. After all Infosys developed it, what objections could the client have.

● b. All code developed as part of a client funded project is the intellectual property of the client and we cannot re-use it in any shape or form. ✓

○ c. You will suggest a feature addition, run an IP check and re-develop the component using Infosys' own guidelines

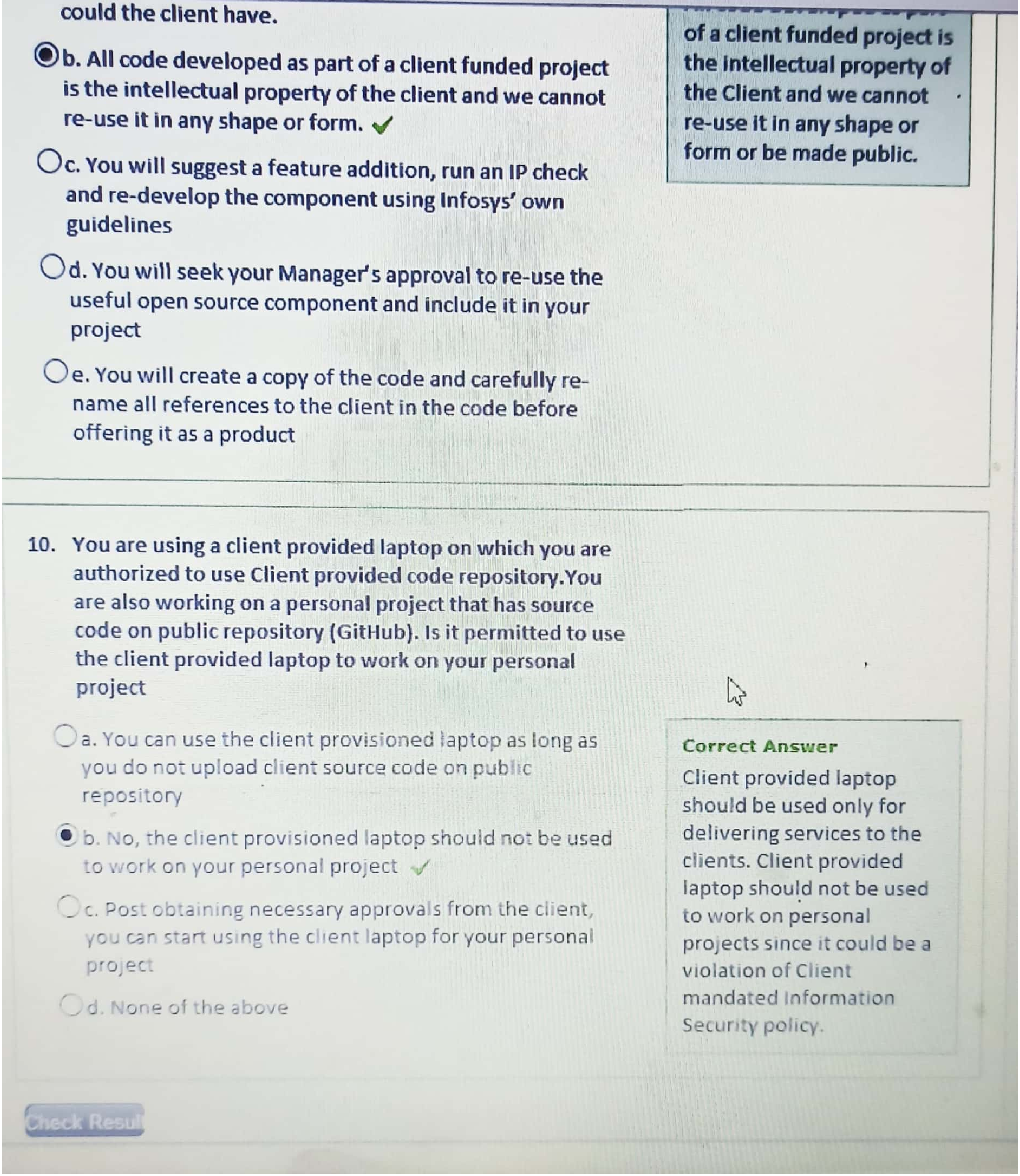
○ d. You will seek your Manager's approval to re-use the useful open source component and include it in your project

○ e. You will create a copy of the code and carefully re-name all references to the client in the code before offering it as a product

Correct Answer

All code developed as part of a client funded project is the intellectual property of the Client and we cannot re-use it in any shape or form or be made public.

10. You are using a client provided laptop on which you are authorized to use Client provided code repository.You are also working on a personal project that has source code on public repository (GitHub). Is it permitted to use



could the client have.

● b. All code developed as part of a client funded project is the intellectual property of the client and we cannot re-use it in any shape or form. ✓

○ c. You will suggest a feature addition, run an IP check and re-develop the component using Infosys' own guidelines

○ d. You will seek your Manager's approval to re-use the useful open source component and include it in your project

○ e. You will create a copy of the code and carefully re-name all references to the client in the code before offering it as a product

of a client funded project is the intellectual property of the Client and we cannot re-use it in any shape or form or be made public.

10. You are using a client provided laptop on which you are authorized to use Client provided code repository.You are also working on a personal project that has source code on public repository (GitHub). Is it permitted to use the client provided laptop to work on your personal project

○ a. You can use the client provisioned laptop as long as you do not upload client source code on public repository

● b. No, the client provisioned laptop should not be used to work on your personal project ✓

○ c. Post obtaining necessary approvals from the client, you can start using the client laptop for your personal project

○ d. None of the above

Correct Answer

Client provided laptop should be used only for delivering services to the clients. Client provided laptop should not be used to work on personal projects since it could be a violation of Client mandated Information Security policy.