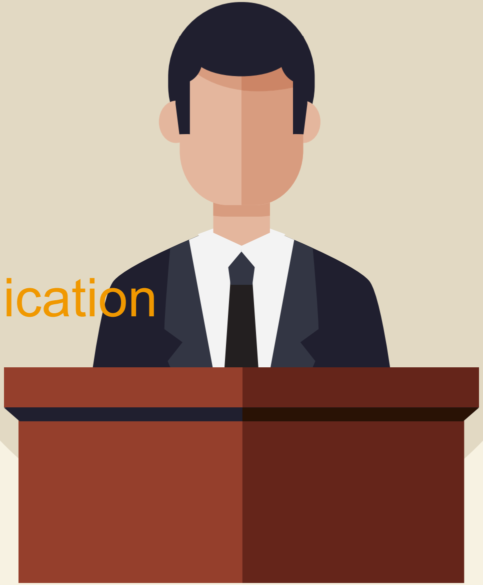
IS4231

Tutorial 5: InfoSec Program at Zoom Video Communication



Team 2

Jerry Ho, Isabella Cheong , Michelle Toh , Kee Kah Lok

Federal Trade Commission (FTC)

Independent agency of the United States governement which aims to protect customers by stopping unfair, deceptive or fraudulent practices in the marketplace

Question1

Considering the misleading and misrepresented information Zoom claimed on its offered videoconferencing services, the FTC commission had reason to believe that Zoom has violated the Federal Trade Commission Act. In Singapore, it would be more likely to be charged under what law?

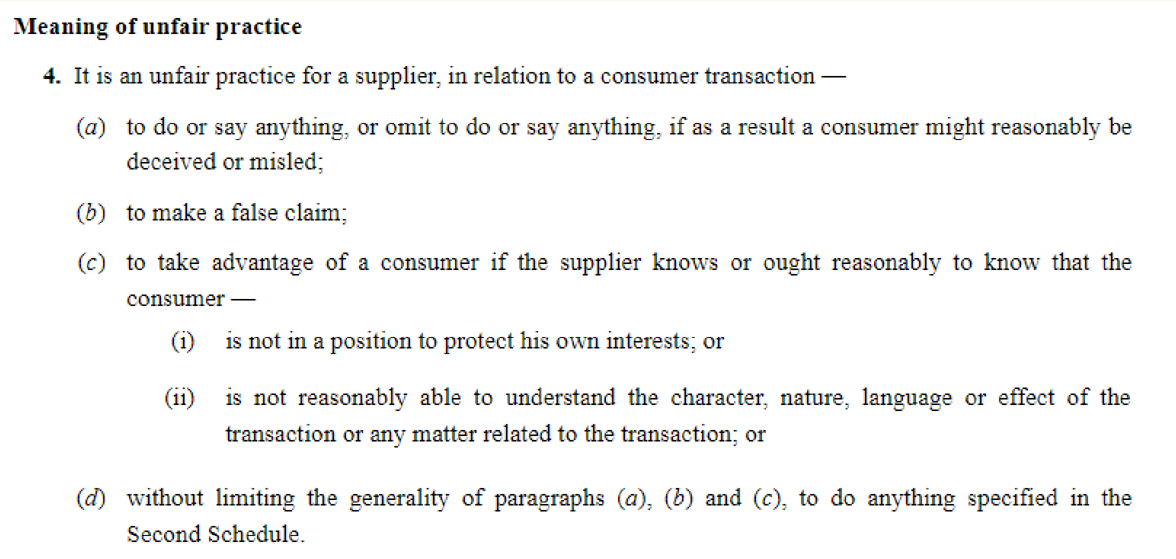
a. PDPA
b. Cybersecurity Act
c. Consumer Protection Act
d. Competition Act

Explanation

Consumer Protection Act

- Protect consumers against unfair practices and to give them additional rights in respecr of the goods that fo not conform to contract, and for matters connected therewith.
- https://www.cccs.gov.sg/legislation/consumer-protection-fair-trading-act

Explanation



Meaning of unfair practice

4. It is an unfair practice for a supplier, in relation to a consumer transaction —

(*a*) to do or say anything, or omit to do or say anything, if as a result a consumer might reasonably be deceived or misled;

(*b*) to make a false claim;

(*c*) to take advantage of a consumer if the supplier knows or ought reasonably to know that the consumer —

(i) is not in a position to protect his own interests; or

(ii) is not reasonably able to understand the character, nature, language or effect of the transaction or any matter related to the transaction; or

(*d*) without limiting the generality of paragraphs (*a*), (*b*) and (*c*), to do anything specified in the Second Schedule.

Question 2

Based on the Final Order from the FTC, what information is not considered as “Covered Information”?

a. Screen name

b. Chat transcripts

c. Processor serial number

d. None of the above

Explanation

From the FTC Final Order:
“Covered Information” means information from or about an individual, including:

c) an email address or other online contact information, such as an instant messaging user identifier or a **screen name**
i) recorded or livestream video or audio content, **chat transcripts**, documents, or any other multimedia content shared by Users during a Meeting
j) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or **processor serial number**

Question 3

In the FTC’s Final Order, the design and implementation of security measures (i.e., policies, procedures, and technical) follows what kind of approach?

a. User based
b. Cost based
c. Risk based
d. Volume based

Explanation

II. Mandated Information Security Program

E. **Design, implement**, maintain, and document **safeguards** that control for the **internal and external risks** Respondent identifies to the security, confidentiality, and integrity of Covered Information identified in response to sub-Provision II.D.

Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information.

Question1

According to the FTC's investigation result, what were the deceptive and unfair practices of Zoom that undermined the security of its users?

Powered by Poll Everywhere

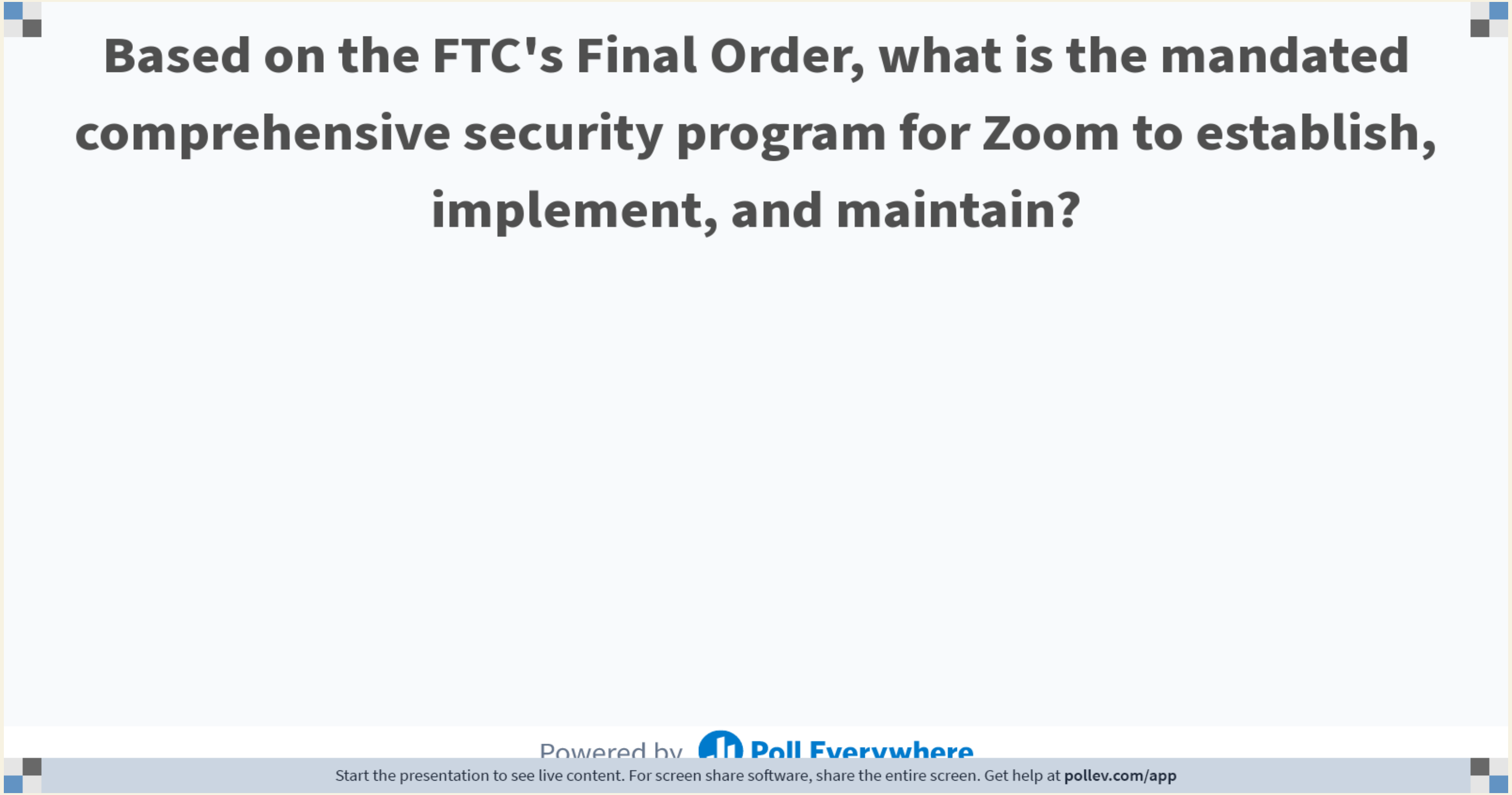
Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question1

According to the FTC’s investigation result, what were the deceptive and unfair practices of Zoom that undermined the security of its users?

- Touted that it offered “end-to-end, 256-bit encryption” to secure users’ communications
- Maintained cryptographic keys that could allow Zoom access to content of customers’ meetings
- Falsely claimed that recorded meetings were encrypted immediately after the meeting ended
- Secretly installed software that remained on computers after the Zoom app was deleted
- Did not implement offsetting measures to protect users’ security, increasing users’ risk of remote video surveillance by strangers.

Question 2



Based on the FTC's Final Order, what is the mandated comprehensive security program for Zoom to establish, implement, and maintain?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 2

Based on the FTC’s Final Order, what is the mandated comprehensive security program for Zoom to establish, implement, and maintain?

A. Document the content, implementation and maintenance of the program

B. For each Covered Incident cover, provide a written program and any material evaluations/material updates to Respondent's board of directors

C. Appoint a qualified employee/employees to coordinate and be responsible for the Program

D. Access and document the internal and external risks to security, confidentiality or integrity of Covered Information after a Covered Incident

E. Design, implement, maintain and document the internal and external risks

F. Access the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality and integrity of Covered Information

Question 2

Based on the FTC's Final Order, what is the mandated comprehensive security program for Zoom to establish, implement, and maintain?

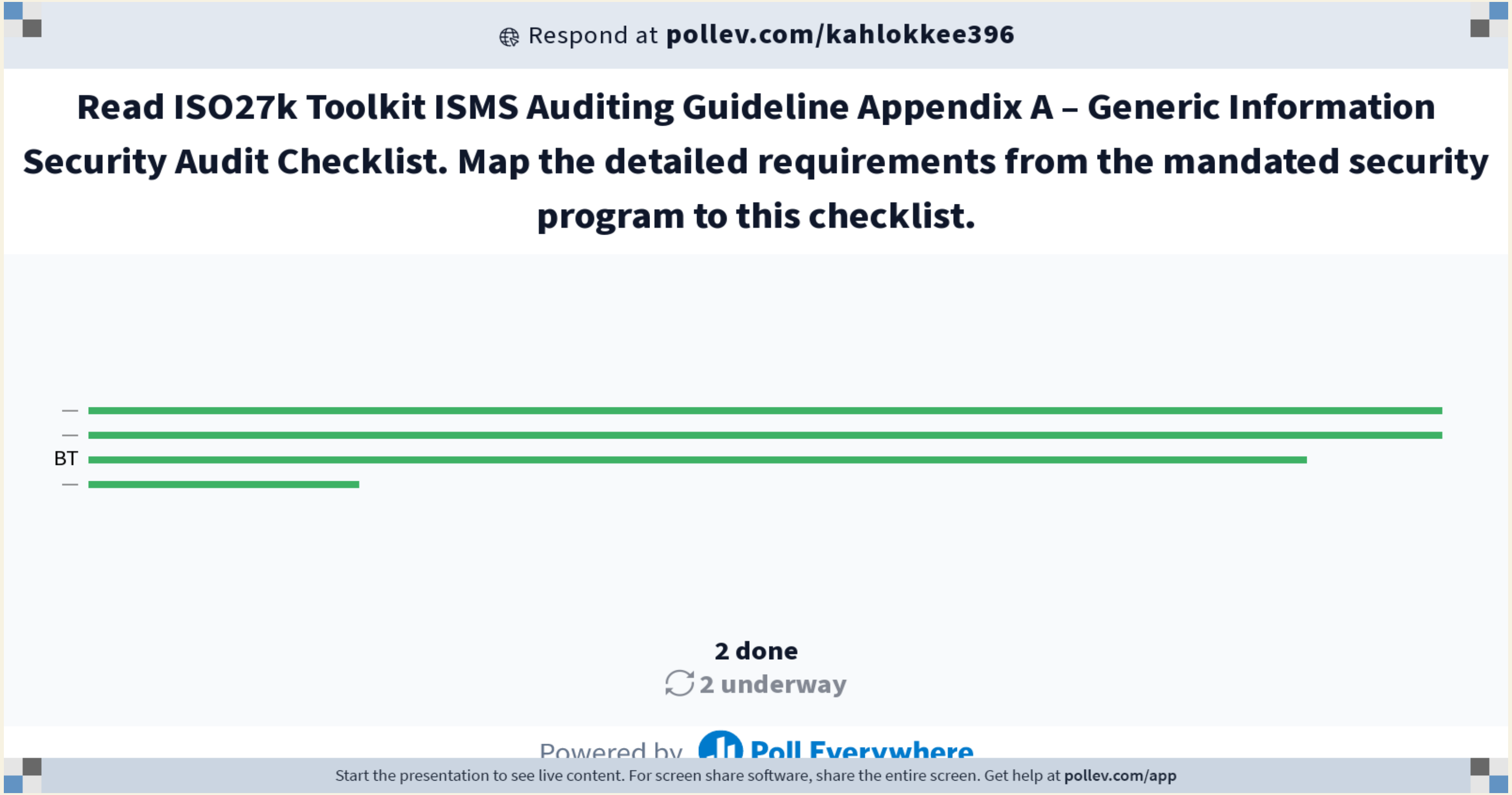
G. Test and monitor the effectiveness of the safeguards and modify the Program based on the results after a Covered Incident

H. Select and retain service providers capable of safeguarding Covered Information they receive

I. Consult with, and seek appropriate guidance from independent 3rd party experts on data protection when establishing, implementing, maintaining and updating the Program

J. Evaluate and adjust the Program in light of any changes to Respondent's operations/business arrangements, a Covered Incident, new or more efficient technology/operational methods

Question3



Respond at **pollev.com/kahlokkee396**

Read ISO27k Toolkit ISMS Auditing Guideline Appendix A – Generic Information Security Audit Checklist. Map the detailed requirements from the mandated security program to this checklist.

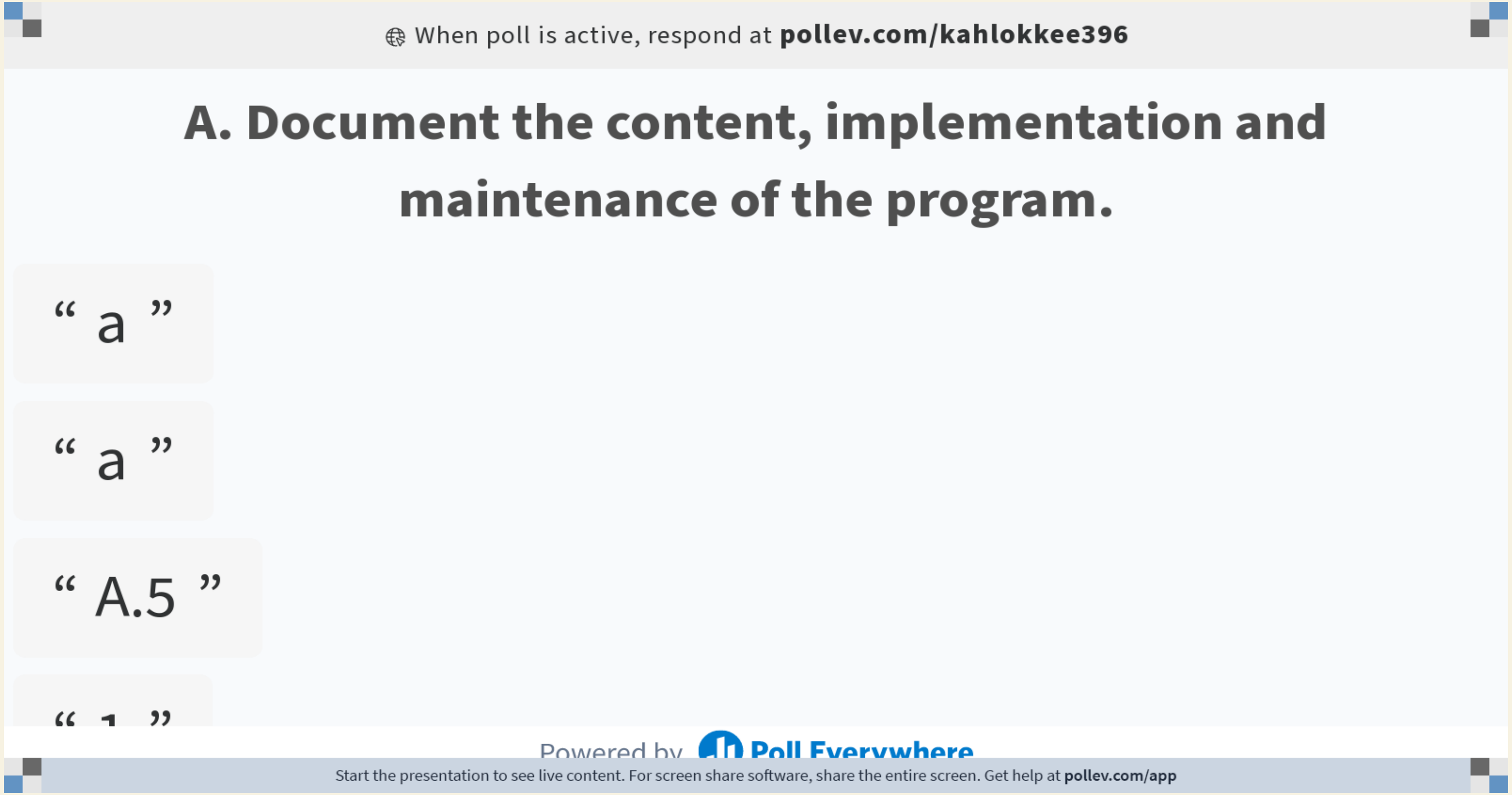
2 done

2 underway

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



When poll is active, respond at **pollev.com/kahlokkee396**

A. Document the content, implementation and maintenance of the program.

“ a ”

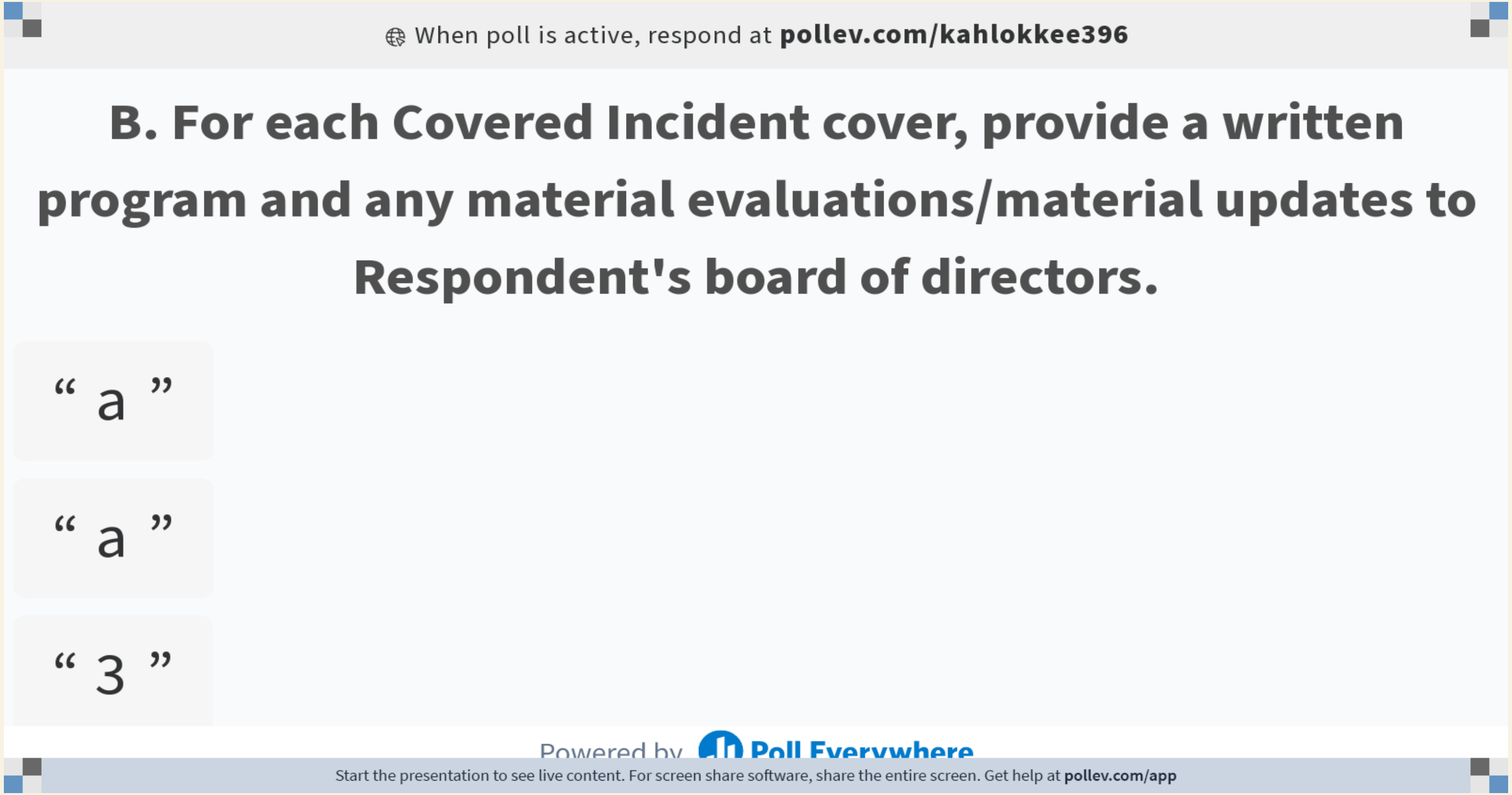
“ a ”

“ A.5 ”

“ 1 ”

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



When poll is active, respond at **pollev.com/kahlokkee396**

B. For each Covered Incident cover, provide a written program and any material evaluations/material updates to Respondent's board of directors.

“ a ”

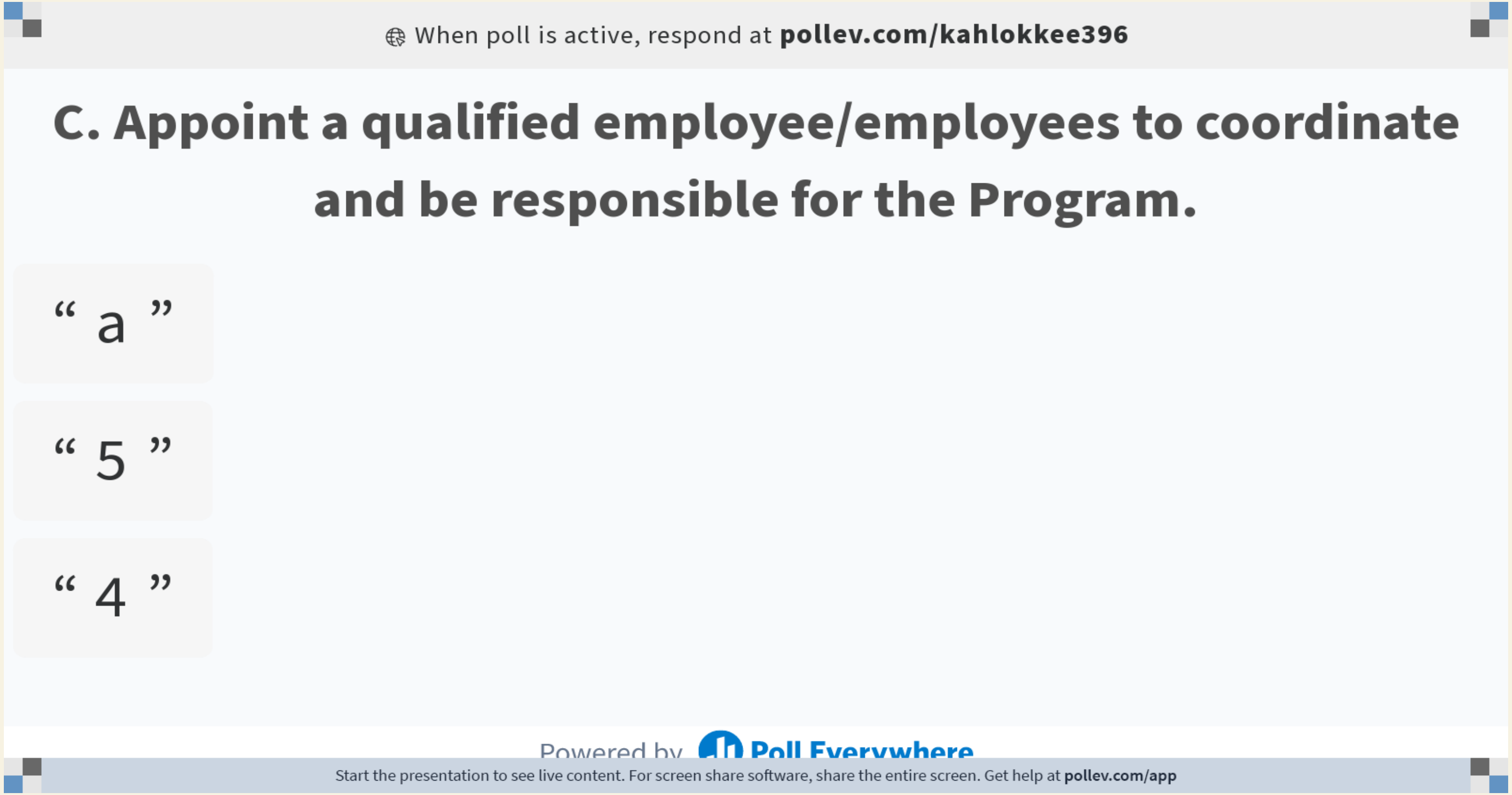
“ a ”

“ 3 ”

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



When poll is active, respond at **pollev.com/kahlokkee396**

C. Appoint a qualified employee/employees to coordinate and be responsible for the Program.

“ a ”

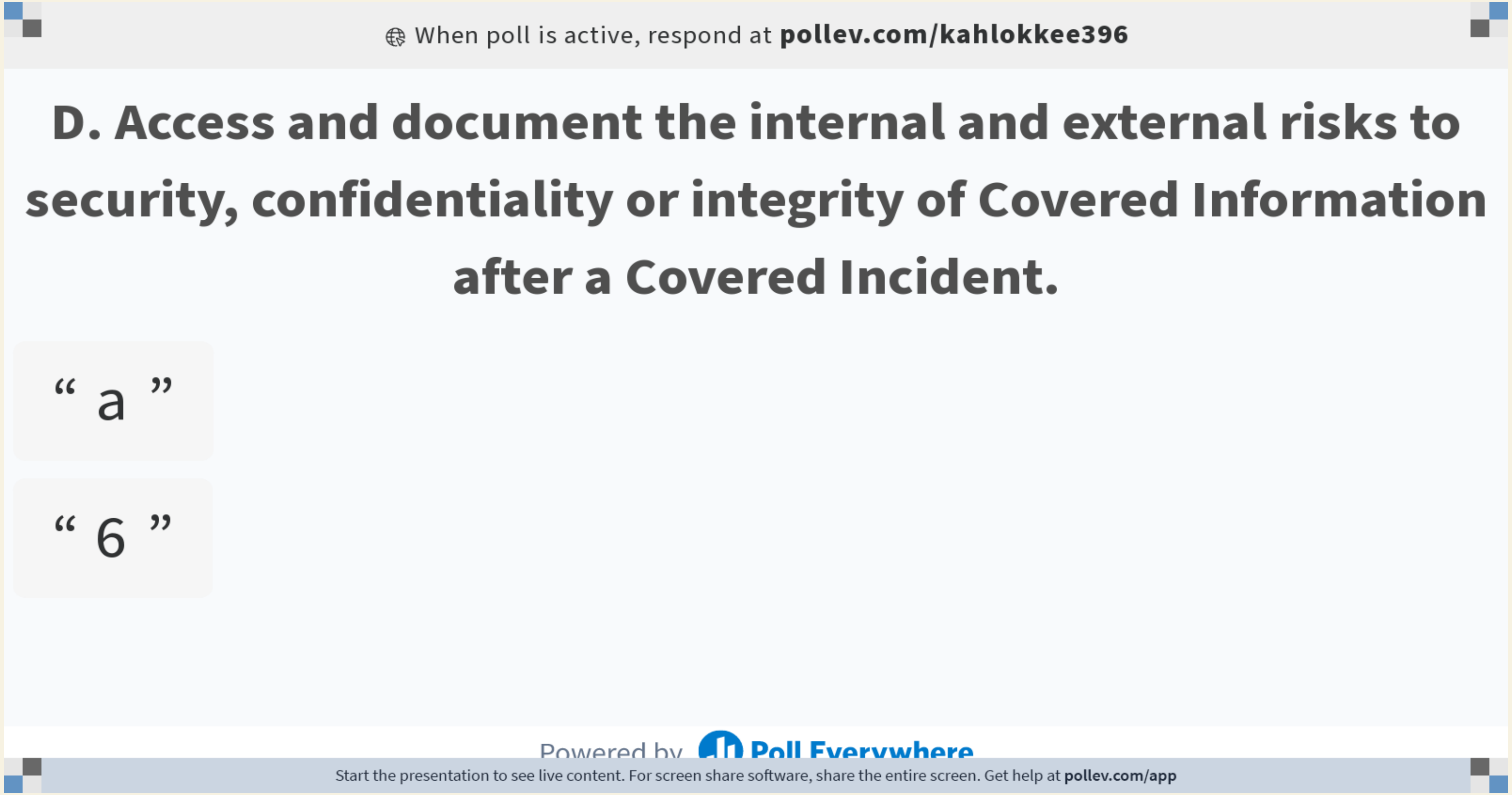
“ 5 ”

“ 4 ”

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



When poll is active, respond at **pollev.com/kahlokkee396**

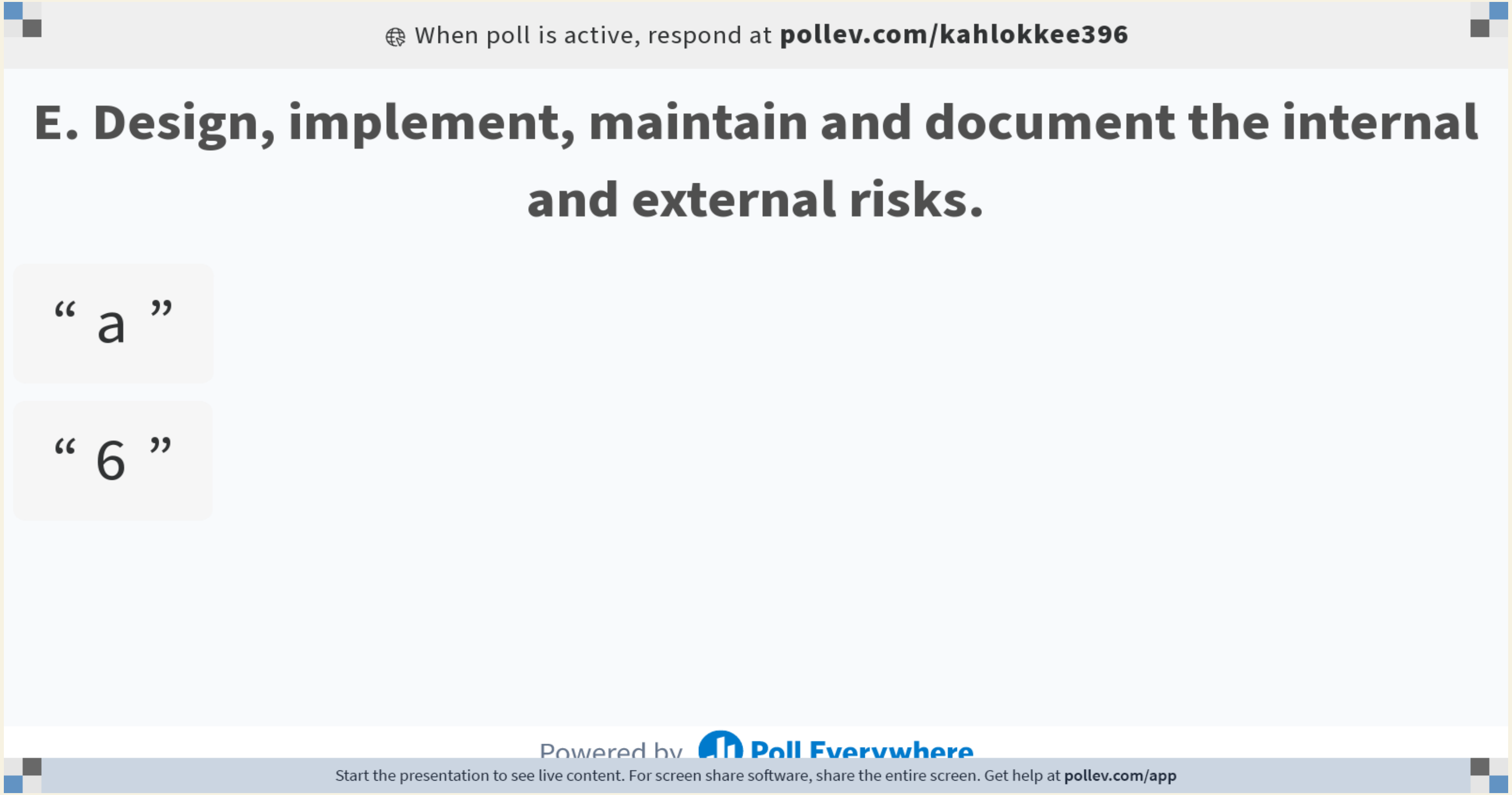
D. Access and document the internal and external risks to security, confidentiality or integrity of Covered Information after a Covered Incident.

“ a ”

“ 6 ”

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



When poll is active, respond at **pollev.com/kahlokkee396**

E. Design, implement, maintain and document the internal and external risks.

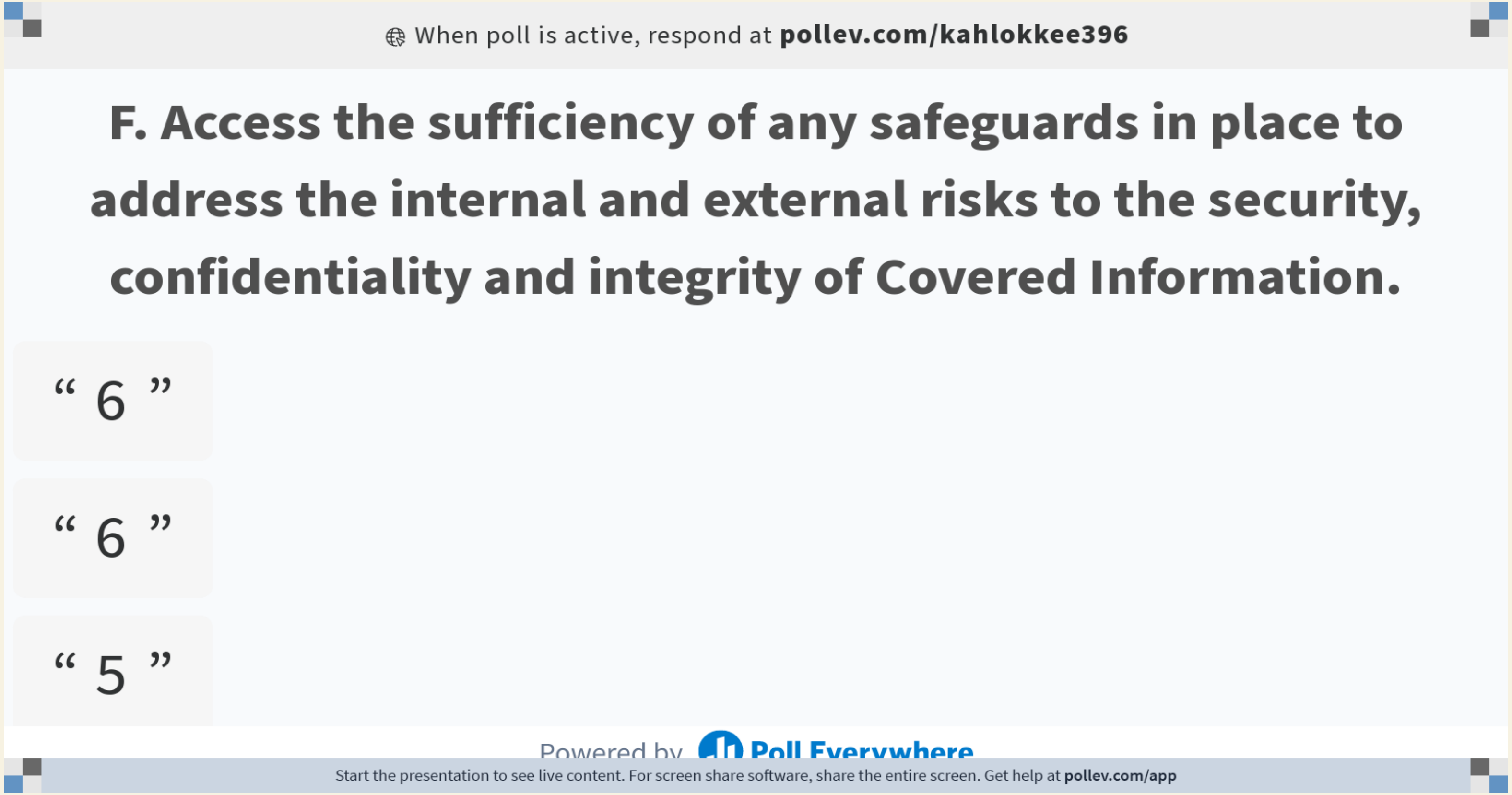
“ a ”

“ 6 ”

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question3



When poll is active, respond at **pollev.com/kahlokkee396**

F. Access the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality and integrity of Covered Information.

“ 6 ”

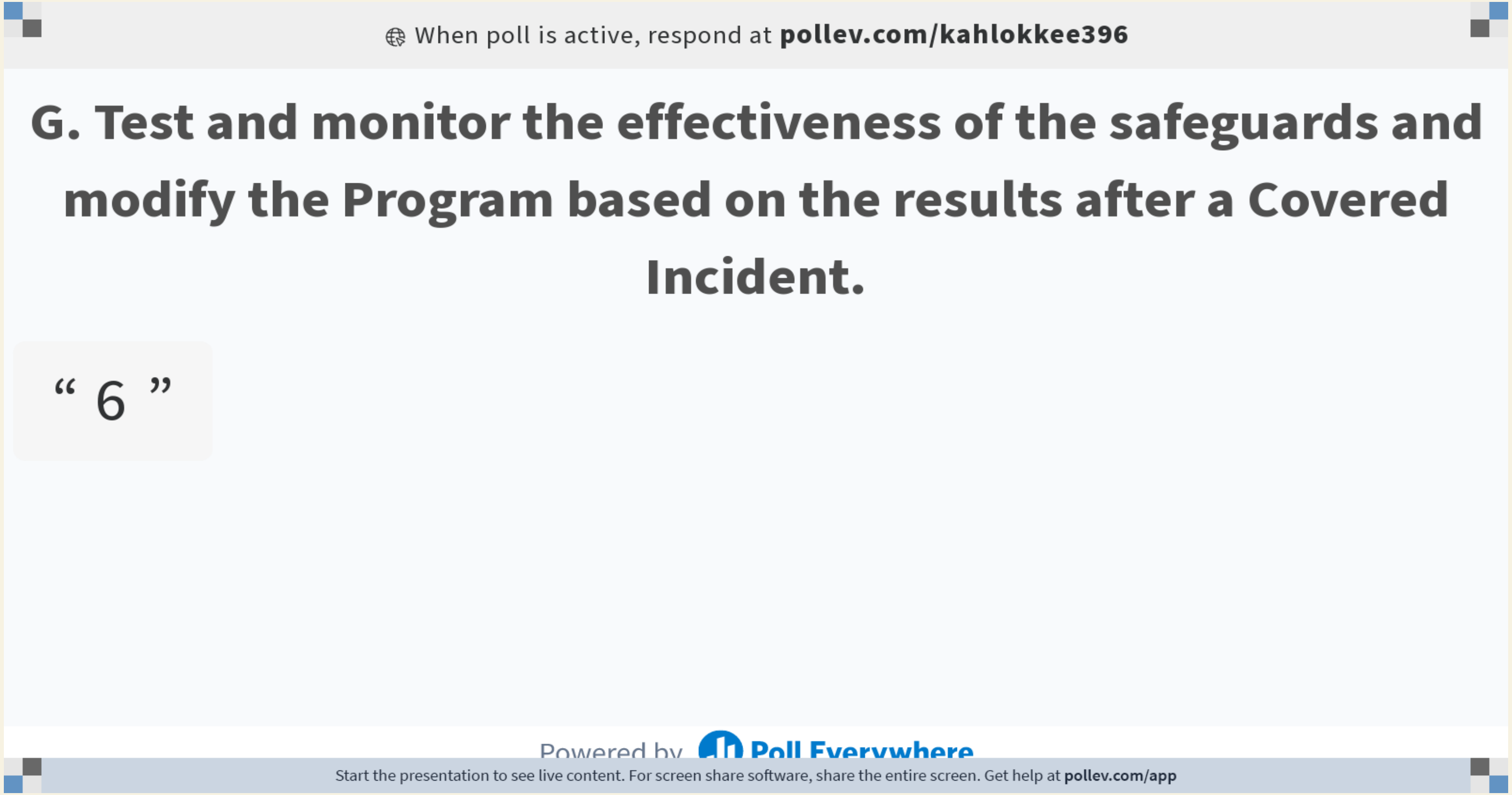
“ 6 ”

“ 5 ”

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question3



When poll is active, respond at **pollev.com/kahlokkee396**

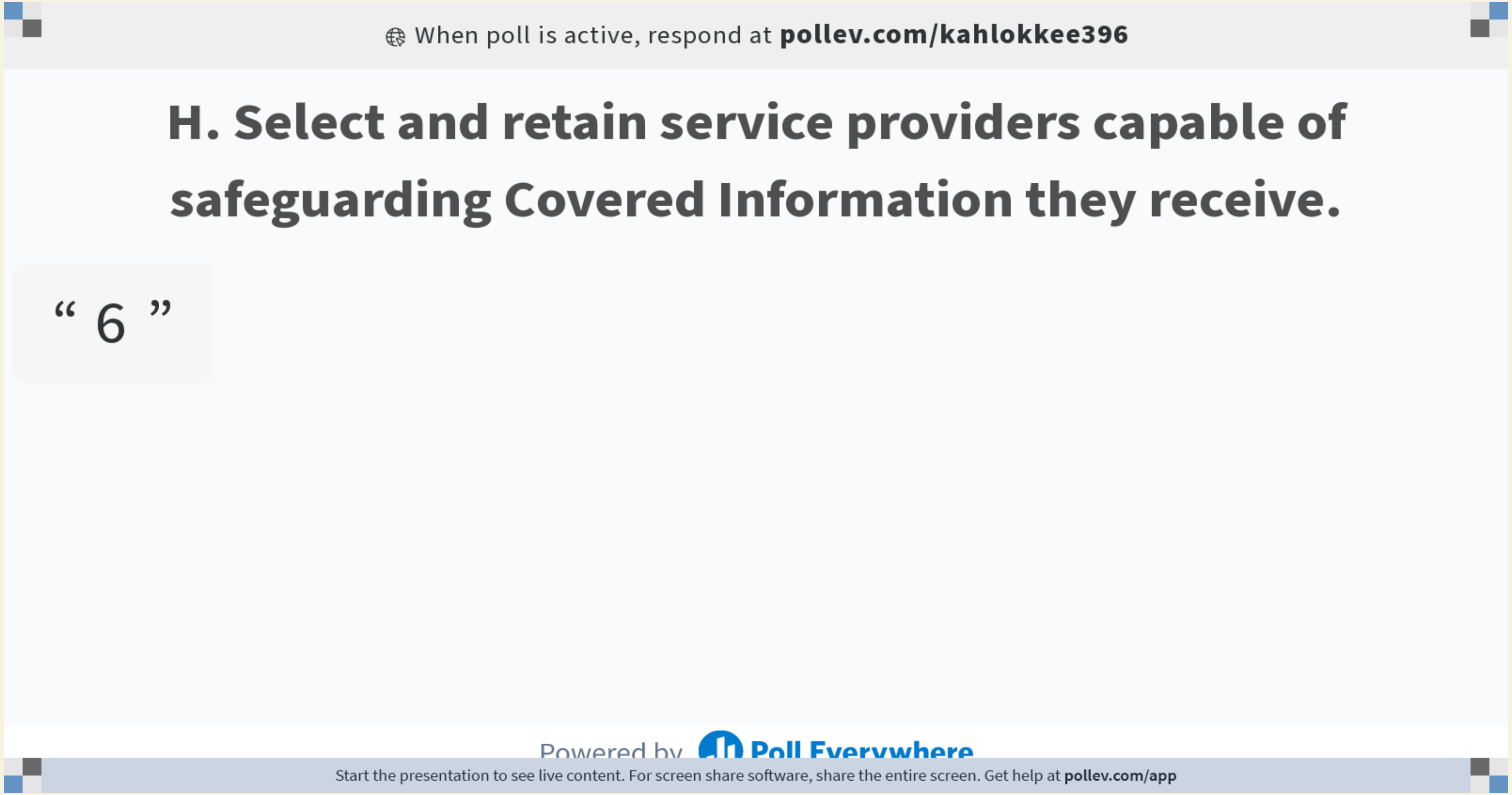
G. Test and monitor the effectiveness of the safeguards and modify the Program based on the results after a Covered Incident.

“ 6 ”

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



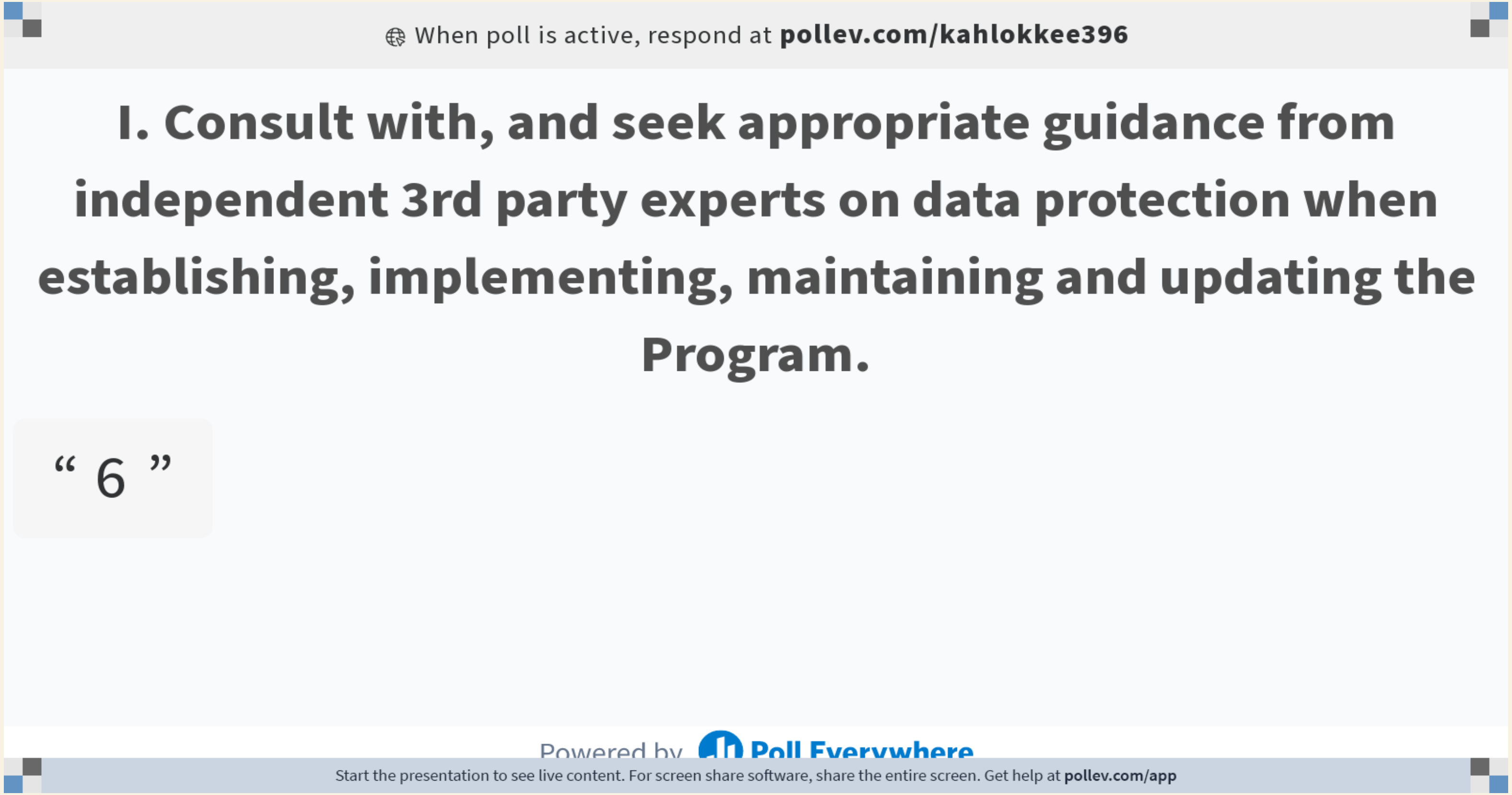
When poll is active, respond at **pollev.com/kahlokkee396**

H. Select and retain service providers capable of safeguarding Covered Information they receive.

“ 6 ”

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question 3



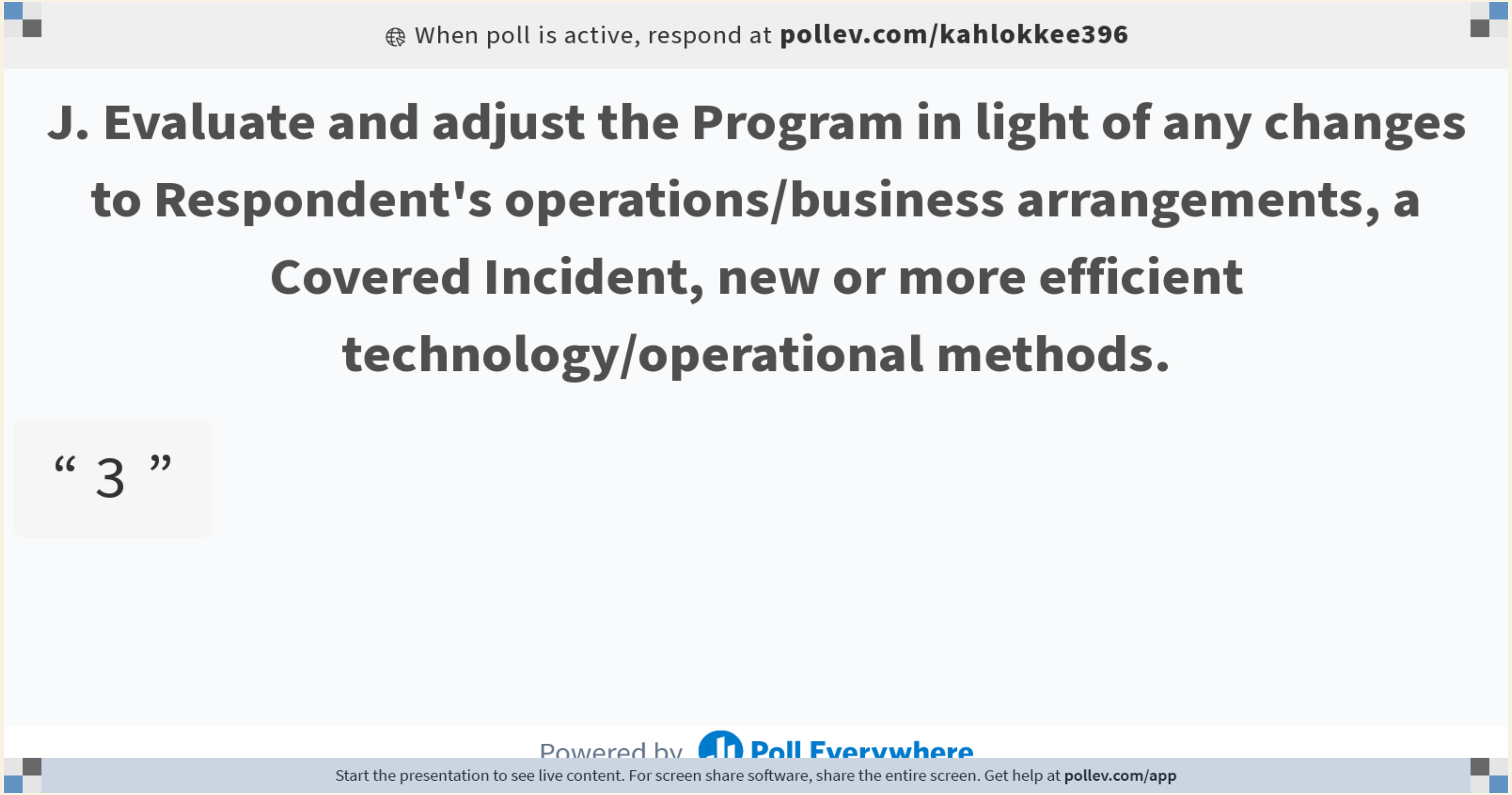
When poll is active, respond at **pollev.com/kahlokkee396**

I. Consult with, and seek appropriate guidance from independent 3rd party experts on data protection when establishing, implementing, maintaining and updating the Program.

“ 6 ”

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question3



When poll is active, respond at **pollev.com/kahlokkee396**

J. Evaluate and adjust the Program in light of any changes to Respondent's operations/business arrangements, a Covered Incident, new or more efficient technology/operational methods.

“ 3 ”

Powered by Poll Everywhere

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Question3

Read ISO27k Toolkit ISMS Auditing Guideline Appendix A – Generic Information Security Audit Checklist. Map the detailed requirements from the mandated security program to this checklist.

A. Document the content, implementation and maintenance of the program. (A.5.1)

B. For each Covered Incident cover, provide a written program and any material evaluations/material updates to Respondent's board of directors. (A.6.1.1)

C. Appoint a qualified employee/employees to coordinate and be responsible for the Program. (A.6.1.1)

D. Access and document the internal and external risks to security, confidentiality or integrity of Covered Information after a Covered Incident. (A.18.2)

E. Design, implement, maintain and document the internal and external risks. (A.5, A.10, A.12)

F. Access the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality and integrity of Covered Information (A.18.2.1)

Question 3

Read ISO27k Toolkit ISMS Auditing Guideline Appendix A – Generic Information Security Audit Checklist. Map the detailed requirements from the mandated security program to this checklist.

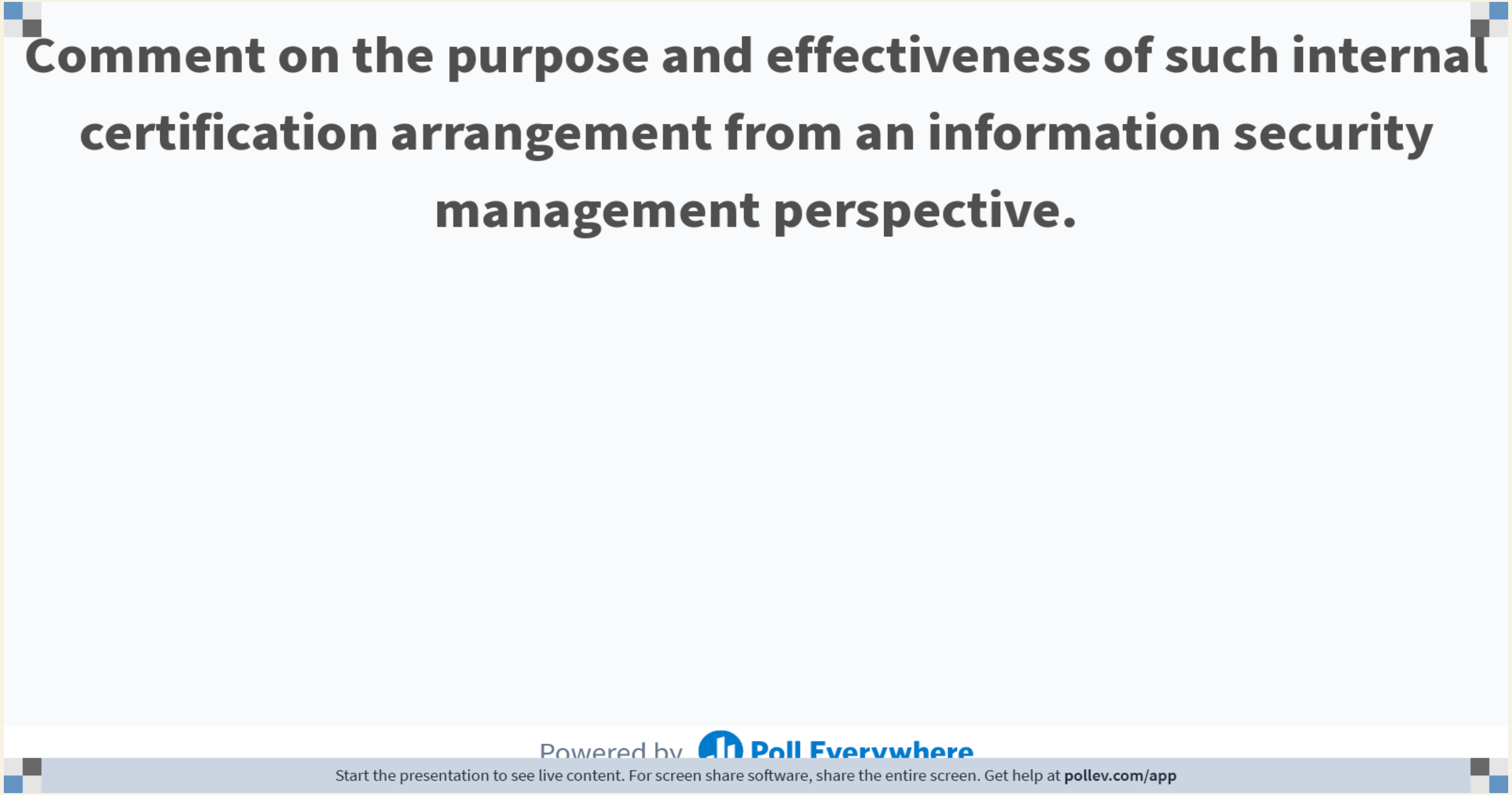
G. Test and monitor the effectiveness of the safeguards and modify the Program based on the results after a Covered Incident. (A.12.6.1, A.14.2.6, A.13.1)

H. Select and retain service providers capable of safeguarding Covered Information they receive. (A.15)

I. Consult with, and seek appropriate guidance from independent 3rd party experts on data protection when establishing, implementing, maintaining and updating the Program. (A.5.1)

J. Evaluate and adjust the Program in light of any changes to Respondent's operations/business arrangements, a Covered Incident, new or more efficient technology/operational methods. (A.5.1.2)

Question 4



Comment on the purpose and effectiveness of such internal certification arrangement from an information security management perspective.

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Explanation

01. Purpose

- To ensure that a high - authority member of the Company is personally aware/involved in the Order
- Establish Accountability

02. Effectiveness

- Developed internal audit process (more audits -> better?)
- C-suite and above is concerned
- Additional manpower required (divert resources from IT security team)
- Length and frequency of audit