



- Expert Verified, Online, **Free**.



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

What is the best way to understand the location, use and importance of personal data within an organization?

- A. By analyzing the data inventory.
- B. By testing the security of data systems.
- C. By evaluating methods for collecting data.
- D. By interviewing employees tasked with data entry.

**Suggested Answer: A**

*Community vote distribution*

A (82%)

C (18%)

🗳️ **alaaz** 7 months, 2 weeks ago

**Selected Answer: A**

best answer

upvoted 1 times

🗳️ **Rocketly** 11 months, 2 weeks ago

**Selected Answer: A**

These things should already be recorded in the data inventory

upvoted 1 times

🗳️ **kevinryt** 1 year, 10 months ago

**Selected Answer: A**

By my trained gpt model

upvoted 2 times

🗳️ **Prateetik** 1 year, 11 months ago

**Selected Answer: A**

Analyzing the data inventory involves creating a comprehensive record of all the personal data that the organization collects, processes, and stores. This includes information about where the data is located, how it is used, who has access to it, and why it is important for the organization's operations. By conducting a thorough data inventory, the organization can gain insights into the scope of its data holdings, identify potential risks and compliance issues, and develop effective data management and protection strategies.

upvoted 1 times

🗳️ **VinFernandesBR** 1 year, 11 months ago

**Selected Answer: A**

data inventory and mapping

upvoted 1 times

🗳️ **EZ2003** 2 years ago

**Selected Answer: A**

data inventory and mapping

upvoted 1 times

🗳️ **Alex951** 2 years ago

**Selected Answer: A**

Data inventory

upvoted 1 times

🗳️ **Vinz\_** 2 years ago

**Selected Answer: C**

My personal view: the correct answer is C) Evaluating methods for collecting data. By doing so, you get an understanding of where data comes from and proceed with your own analysis.

A) is wrong because data inventory might be either not present or inaccurate, and this is the case for the majority of the times in real scenarios.

B) is wrong, security of data systems doesn't provide clues on the applicable legislations.

D) is wrong because employees tasked with data entry might not be knowledgeable on where data comes from, how it is transmitted (e.g., unencrypted) and where is stored.

upvoted 2 times

  **bilgecell** 2 years, 2 months ago

**Selected Answer: A**

By analysing data inventory

upvoted 1 times

What are you doing if you succumb to "overgeneralization" when analyzing data from metrics?

- A. Using data that is too broad to capture specific meanings.
- B. Possessing too many types of data to perform a valid analysis.
- C. Using limited data in an attempt to support broad conclusions.
- D. Trying to use several measurements to gauge one aspect of a program.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: C**

This is the definition of overgeneralisation  
upvoted 1 times

🗳️ 👤 **BevMe** 1 year, 1 month ago

**Selected Answer: C**

'Overgeneralization' in data analysis occurs when conclusions are extrapolated beyond the scope of the available evidence.  
upvoted 1 times

🗳️ 👤 **giomike** 1 year, 5 months ago

Answer is C:\ Overgeneralization in data analysis occurs when conclusions or insights are drawn from a dataset that are too broad or universal, based on a limited sample or specific conditions.  
upvoted 1 times

🗳️ 👤 **kevinryt** 1 year, 10 months ago

**Selected Answer: C**

By my trained gpt model  
upvoted 2 times

🗳️ 👤 **baranikumar\_v** 1 year, 11 months ago

C. We may, for example, predict the outcome of something based on just one instance of it: After going on a job interview and finding out we didn't get the job, we conclude we'll never get a job (overgeneralizing) and feel hopeless about our career, leading to sadness and depression  
upvoted 3 times

🗳️ 👤 **EZ2003** 2 years ago

**Selected Answer: C**

Overgeneralization happens when you assume what you are seeing in your dataset is what you would see if you looked any other dataset meant to assess the same information, despite the fact that your data is very small or sometimes it's selected subset.  
upvoted 1 times

🗳️ 👤 **mgmferreira** 2 years, 1 month ago

**Selected Answer: C**

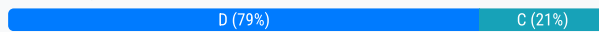
C. Overgeneralization. This occurs when inferences are made concerning a general data population that leads to poor conclusions; for example, extrapolating limited experiences and evidence to broad generalizations  
upvoted 3 times

In addition to regulatory requirements and business practices, what important factors must a global privacy strategy consider?

- A. Monetary exchange.
- B. Geographic features.
- C. Political history.
- D. Cultural norms.

**Suggested Answer: D**

*Community vote distribution*



**alaaz** 7 months, 2 weeks ago

**Selected Answer: D**

D is correct

upvoted 1 times

**Awinfred** 11 months ago

The answer is B

upvoted 1 times

**Rocketly** 11 months, 2 weeks ago

**Selected Answer: D**

D is referred to as a factor to consider a few times within the textbook. The other options are not mentioned

upvoted 2 times

**giomike** 1 year, 5 months ago

The answer is D: Cultural attitudes towards privacy can vary significantly across regions. A global privacy strategy should be sensitive to cultural differences and ethical considerations related to privacy. What is acceptable in one culture may be considered invasive in another.

upvoted 3 times

**carlosbui** 1 year, 8 months ago

Should be D

upvoted 2 times

**kevinryt** 1 year, 10 months ago

**Selected Answer: D**

By my trained gpt model

upvoted 2 times

**creativesyde** 1 year, 11 months ago

**Selected Answer: D**

cultural norms

upvoted 2 times

**EZ2003** 2 years ago

**Selected Answer: D**

culture norms

upvoted 2 times

**DracoL** 2 years, 1 month ago

**Selected Answer: D**

click wrongly. Shoul dbe D

upvoted 2 times

**DracoL** 2 years, 1 month ago

**Selected Answer: C**

Cultural Norm should be the correct answer. Someone replied As everyone has already said, it's definitely D. To put it into context, the CIPM highlights the importance of understanding the context you are working in, i.e. not seeing data protection as a standalone issue, but something which responds

to the context of the organisation you are working for. So issues like the wider organisational context, type of business, cultural norms, risk appetite of your organisation, and so on, are all factors in ensuring that the privacy program is positioned to respond to those needs as well as the more privacy/data protection specific legal and regulatory requirements.

upvoted 3 times


What have experts identified as an important trend in privacy program development?

- A. The narrowing of regulatory definitions of personal information.
- B. The rollback of ambitious programs due to budgetary restraints.
- C. The movement beyond crisis management to proactive prevention.
- D. The stabilization of programs as the pace of new legal mandates slows.

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **Rocketly** 11 months, 2 weeks ago

**Selected Answer:** C

This is mentioned in the textbook

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What step in the system development process did Manasa skip?

- A. Obtain express written consent from users of the Handy Helper regarding marketing.
- B. Work with Sanjay to review any necessary privacy requirements to be built into the product.
- C. Certify that the Handy Helper meets the requirements of the EU-US Privacy Shield Framework.
- D. Build the artificial intelligence feature so that users would not have to input sensitive information into the Handy Helper.

**Suggested Answer: B**

Community vote distribution

B (100%)

  **tonik** Highly Voted 2 years, 2 months ago

I suggest B

upvoted 6 times

  **Jenkins3mol** Most Recent 2 months ago

**Selected Answer: B**

But this is so painfully wordy...

upvoted 1 times

  **alaaz** 7 months, 2 weeks ago

**Selected Answer: B**

Privacy should be built-in.



upvoted 1 times

  **Rocketly** 11 months, 2 weeks ago

**Selected Answer: B**

Privacy by Design (PbD)

upvoted 1 times

  **carlosbui** 1 year, 8 months ago

should be B

upvoted 2 times

  **baranikumar\_v** 1 year, 11 months ago

B. Privacy should be built-in.



upvoted 3 times

  **PattoDPO** 2 years ago

B is the most appropriate answer.

upvoted 2 times

  **Boats** 2 years ago

**Selected Answer: B**

The principles of privacy by design offer an outstanding starting point for integrating privacy thinking into a systems engineering practice. Privacy and security professionals should work together to communicate to all relevant stakeholders the importance of integrating these principles into the work of the organization.

Chapple, Mike; Shelley, Joe. IAPP CIPM Certified Information Privacy Manager Study Guide (p. 140). Wiley. Kindle Edition.

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What administrative safeguards should be implemented to protect the collected data while in use by Manasa and her product management team?

- A. Document the data flows for the collected data.
- B. Conduct a Privacy Impact Assessment (PIA) to evaluate the risks involved.
- C. Implement a policy restricting data access on a "need to know" basis.
- D. Limit data transfers to the US by keeping data collected in Europe within a local data center.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ **Rocketly** 11 months, 2 weeks ago

**Selected Answer: C**

Administrative safeguard = access controls  
upvoted 1 times

🗳️ **BevMe** 1 year, 1 month ago

**Selected Answer: C**

A, B and D are important, but not directly relevant to protecting the data to the extent that C is.  
upvoted 1 times

🗳️ **baranikumar\_v** 1 year, 11 months ago

C. Detail need to know on what basis, the access to the collected data shall be given  
upvoted 3 times

🗳️ **PattoDPO** 2 years ago

C - most correct answer  
upvoted 2 times

🗳️ **DracoL** 2 years, 2 months ago



**Selected Answer: C**

The talk is administrative safeguard. Document the flow doesnt safeguard anything but understand the flow. I am suggesting C  
upvoted 3 times

🗳️ **mansour975** 2 years, 2 months ago

I agree with you C is the most correct answer

upvoted 2 times

  **tonik** 2 years, 2 months ago

Maybe C

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What element of the Privacy by Design (PbD) framework might the Handy Helper violate?

- A. Failure to obtain opt-in consent to marketing.
- B. Failure to observe data localization requirements.
- C. Failure to implement the least privilege access standard.
- D. Failure to integrate privacy throughout the system development life cycle.

**Suggested Answer: D**


Community vote distribution

D (100%)

 **KennyDo** 8 months ago

**Selected Answer: D**

Goodluck to the cyber team who plans to take the exam this week  
upvoted 2 times

 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: D**

D describes the PbD principle. Data localisation relates more to international data transfer requirements under GDPR  
upvoted 1 times

 **BevMe** 1 year, 1 month ago

**Selected Answer: D**

PbD is about integrating privacy requirements at the design phase of new systems, processes and projects undertaken.  
upvoted 1 times

 **baranikumar\_v** 1 year, 11 months ago

D. privacy should have integrated as part of the product/system development life cycle.  
upvoted 2 times

 **Alex951** 2 years ago

**Selected Answer: D**

should be D  
upvoted 3 times

 **tonik** 2 years, 2 months ago



Agree with D

upvoted 2 times

  **Boerenkool** 2 years, 4 months ago

Should be D

upvoted 2 times

  **EniJack** 2 years, 5 months ago

**Selected Answer: D**

i dont have any comments

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What can Sanjay do to minimize the risks of offering the product in Europe?

- A. Sanjay should advise the distributor that Omnipresent Omnimedia has certified to the Privacy Shield Framework and there should be no issues.
- B. Sanjay should work with Manasa to review and remediate the Handy Helper as a gating item before it is released.
- C. Sanjay should document the data life cycle of the data collected by the Handy Helper.
- D. Sanjay should write a privacy policy to include with the Handy Helper user guide.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: B**

The product should not be launched until it has been assessed as GDPR compliant  
upvoted 1 times

🗳️ 👤 **BevMe** 1 year, 1 month ago

**Selected Answer: B**

The correct answer is B  
upvoted 1 times

🗳️ 👤 **saleem4u** 1 year, 7 months ago

B. Sanjay should work with Manasa to review and remediate the Handy Helper as a gating item before it is released.  
upvoted 1 times

🗳️ 👤 **baranikumar\_v** 1 year, 11 months ago

B. First assess the gap to understand whether the app is fit to release in EU considering the privacy norms in that region.  
upvoted 2 times

🗳️ 👤 **\_sleepless770** 2 years ago

**Selected Answer: B**

ANSWER IS B  
upvoted 1 times

🗳️ 👤 **tonik** 2 years, 2 months ago

Maybe B

upvoted 1 times

Which statement is FALSE regarding the use of technical security controls?

- A. Technical security controls are part of a data governance strategy.
- B. Technical security controls deployed for one jurisdiction often satisfy another jurisdiction.
- C. Most privacy legislation lists the types of technical security controls that must be implemented.
- D. A person with security knowledge should be involved with the deployment of technical security controls.

**Suggested Answer: C**

Community vote distribution

C (82%)

Other

🗳️ 👤 **7b9a452** 10 months ago

The most logical answer is C.  
upvoted 1 times

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: C**

It would not be practical for laws to list specific technical measures, as these evolve over time  
upvoted 1 times

🗳️ 👤 **BevMe** 1 year, 1 month ago

**Selected Answer: C**

Most privacy laws focus on outcomes e.g., ensuring data security rather than specifying exact technical security measures. This allows organisations the flexibility to choose controls that would work best for their environment.  
upvoted 4 times

🗳️ 👤 **MaritzTee** 1 year, 1 month ago

The correct answer is C. Most privacy legislation does not specify the exact types of technical security controls that must be implemented. Instead, they often require that organizations implement "appropriate" or "reasonable" security measures, leaving the specifics up to the organizations to determine based on their particular circumstances and risks.  
upvoted 1 times

🗳️ 👤 **katizeti** 1 year, 4 months ago

Both B and C options are incorrect.  
upvoted 1 times

🗳️ 👤 **giomike** 1 year, 5 months ago

C. Most privacy legislation lists the types of technical security controls that must be implemented.

Explanation: While privacy legislation often requires organizations to protect the privacy and security of personal data, it typically does not prescribe specific technical security controls. Instead, it often outlines general principles and requirements for safeguarding information. The choice of specific technical security controls is left to the organizations themselves, considering their unique circumstances and the nature of the data they handle.  
upvoted 4 times

🗳️ 👤 **krishccie** 1 year, 6 months ago

**Selected Answer: B**

Jurisdictions might have different controls requirements  
upvoted 1 times

🗳️ 👤 **drluvkashyap** 1 year, 9 months ago

The false statement regarding the use of technical security controls is: B. Technical security controls deployed for one jurisdiction often satisfy another jurisdiction.

This is false because technical security controls that are required in one jurisdiction may not be sufficient to meet the requirements of another jurisdiction. For example, the European Union's General Data Protection Regulation (GDPR) has stricter requirements for technical security controls than the United States' Health Insurance Portability and Accountability Act (HIPAA).  
upvoted 1 times



🗨️ 👤 **DracoL** 2 years, 1 month ago

**Selected Answer: C**

Answer is C because the question ask for False about data security. While Technical Security Controls are part of data goverance strategy but it in most legislation never really list what technical control required.

"C. Most privacy legislation lists the types of technical security controls that must be implemented. "

upvoted 4 times

🗨️ 👤 **giomike** 2 years, 1 month ago

While technical security controls play a crucial role in safeguarding data, they are not synonymous with data governance

upvoted 1 times

🗨️ 👤 **DracoL** 2 years, 2 months ago

**Selected Answer: A**

Technical Security Controls are part of data governance strategy

upvoted 1 times

🗨️ 👤 **mansour975** 2 years, 2 months ago

C maybe the correct answer

upvoted 2 times

🗨️ 👤 **tonik** 2 years, 2 months ago

A or C

upvoted 1 times

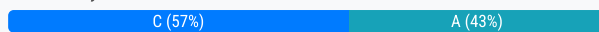
An organization's privacy officer was just notified by the benefits manager that she accidentally sent out the retirement enrollment report of all employees to a wrong vendor.

Which of the following actions should the privacy officer take first?

- A. Perform a risk of harm analysis.
- B. Report the incident to law enforcement.
- C. Contact the recipient to delete the email.
- D. Send firm-wide email notification to employees.

**Suggested Answer: C**

Community vote distribution



**giomike** Highly Voted 1 year, 5 months ago

The answer is C: The privacy officer should work with the benefits manager to contain the breach promptly. This may involve contacting the vendor and requesting them to delete or secure the data immediately.

upvoted 5 times

**Jenkins3mol** Most Recent 2 months ago

**Selected Answer: C**

Contain the risk first. The analysis of harm can happen later.

upvoted 1 times

**ShadyB** 4 months, 3 weeks ago

**Selected Answer: C**

The privacy officer should first C. Contact the recipient to delete the email.

Here's why:

Immediate Mitigation: The priority is to minimize the potential damage. Contacting the vendor to request immediate deletion of the email is the most direct and immediate way to attempt to contain the breach.

Time Sensitivity: Every moment that the data is in the wrong hands increases the risk. Contacting the recipient is the fastest action to take.

Here's why the other options are not the first step:

A. Perform a risk of harm analysis: A risk of harm analysis is a necessary step, but it comes after attempting to contain the breach.

upvoted 2 times

**Drackos2** 6 months, 3 weeks ago

**Selected Answer: A**

Risk analysis should be the first step and then containment of the information.

upvoted 4 times

**Rocketly** 11 months, 2 weeks ago

**Selected Answer: C**

Act immediately to mitigate and contain the breach. Then move onto other actions e.g. assessing the potential harm

upvoted 1 times

**Jutt** 1 year ago

It should be A to determine the harm first.

upvoted 2 times

**BevMe** 1 year, 1 month ago

**Selected Answer: C**

The first priority in such situations is to mitigate any potential harm by containing the breach.

upvoted 2 times

**humhain** 1 year, 4 months ago

Selected Answer: A

Risk Analysis

upvoted 2 times

🗉 👤 **Cock** 1 year, 9 months ago

Selected Answer: C

I vote for c

upvoted 2 times

🗉 👤 **Gh789** 1 year, 11 months ago

C - data encryption is not clarified, the immediate action should be containment

upvoted 2 times

🗉 👤 **emily0922** 1 year, 11 months ago

Should be C, to secure operations and make sure no additional data is lost first

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production – not data processing – and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth – his uncle's vice president and longtime confidante – wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check. Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.



To improve the facility's system of data security, Anton should consider following through with the plan for which of the following?

- A. Customer communication.
- B. Employee access to electronic storage.
- C. Employee advisement regarding legal matters.
- D. Controlled access at the company headquarters.

**Suggested Answer: D**

Community vote distribution


D (100%)

  **Dhrumal** 7 months, 2 weeks ago

**Selected Answer: D**

Question asked 'facility's system security' hence answering D.

upvoted 1 times

  **Rocketly** 11 months, 2 weeks ago

**Selected Answer: D**

Access control should be an immediate priority - this will also help mitigate security risks until files can be digitalised

upvoted 1 times

  **MaritzTee** 1 year, 1 month ago

D is correct. Implementing controlled access at the company headquarters will help secure the physical premises, ensuring that only authorized personnel can access areas where sensitive information is stored. This is a fundamental step in protecting against data breaches and aligns with Anton's goal of guaranteeing zero loss of personal information. While the other options are important, controlled access addresses the immediate concern of physical security, which is critical given the disorganized state of the company's data storage.

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production – not data processing – and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth – his uncle's vice president and longtime confidante – wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check. Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

Which of Anton's plans for improving the data management of the company is most unachievable?

- A. His initiative to achieve regulatory compliance.
- B. His intention to transition to electronic storage.
- C. His objective for zero loss of personal information.
- D. His intention to send notice letters to customers and employees.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Dhrumal** 7 months, 2 weeks ago

**Selected Answer: C**

zero risk of privacy breach is an ideal scenario.

upvoted 1 times

🗳️ 👤 **zxybc61** 1 year, 5 months ago

**Selected Answer: C**

C is correct

upvoted 2 times

🗳️ 👤 **baranikumar\_v** 1 year, 11 months ago

C. Zero privacy breach is something that can't be guaranteed.

upvoted 3 times

🗳️ 👤 **PattoDPO** 2 years ago

C - correct!

upvoted 3 times

🗳️ 👤 **tonik** 2 years, 2 months ago

One more vote for C

upvoted 3 times

  **Boerenkool** 2 years, 4 months ago

C is correct

upvoted 2 times

  **Larryqwe** 2 years, 4 months ago

Answer C is correct

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production – not data processing – and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth – his uncle's vice president and longtime confidante – wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check. Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.


Which important principle of Data Lifecycle Management (DLM) will most likely be compromised if Anton executes his plan to limit data access to himself and Kenneth?

- A. Practicing data minimalism.
- B. Ensuring data retrievability.
- C. Implementing clear policies.
- D. Ensuring adequacy of infrastructure.

**Suggested Answer: B**


Community vote distribution

B (100%)

 **emily0922** Highly Voted 1 year, 4 months ago

B, according to IAPP, the 11 DLM elements are Ent Objectives, Minimalism, Simplicity of procedures and Training, Adequacy of Infrastructure, Auditability, Authenticity and Accuracy of One's own Records, Distribution Controls, Info Sec, Consistency of Policies, Enforcement and Retrievability. In this case it will affect Retrievability.

upvoted 5 times

 **humhain** Most Recent 10 months, 3 weeks ago

**Selected Answer: B**

Data retrievability refers to the ability to access and use data when needed for business purposes or legal obligations<sup>1</sup> It involves maintaining the availability, integrity, and usability of data throughout its lifecycle<sup>2</sup> However, if Anton restricts data access to only himself and Kenneth, he will create a single point of failure and a bottleneck for data retrieval. This could pose several risks and challenges for the company, such as:

Losing data if Anton or Kenneth forgets the password or leaves the company without sharing it with others.

Delaying data retrieval if Anton or Kenneth is unavailable or unresponsive when someone else needs the data urgently.

Violating data protection laws or regulations that require data access by certain parties or authorities under certain circumstances.

Reducing data quality or accuracy if Anton or Kenneth fails to update or maintain the data properly.



Missing business opportunities or insights if Anton or Kenneth does not share the data with other relevant stakeholders or departments.

upvoted 4 times

  **Alex951** 1 year, 7 months ago

I suggest B

upvoted 3 times

  **DracoL** 1 year, 8 months ago

**Selected Answer: B**

look like B cause only 2 person can retrieve data.

upvoted 3 times

  **Boerenkool** 1 year, 10 months ago

Should be B

upvoted 3 times

  **Larryqwe** 1 year, 11 months ago

Answer is b

upvoted 4 times



## SCENARIO -

Please use the following to answer the next question:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production – not data processing – and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth – his uncle's vice president and longtime confidante – wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check. Documentation of this analysis will show auditors due diligence.

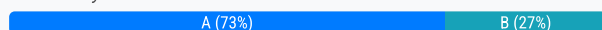
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding?

- A. The timeline for monitoring.
- B. The method of recordkeeping.
- C. The use of internal employees.
- D. The type of required qualifications.

**Suggested Answer: A**

Community vote distribution



**ShadyB** 4 months, 3 weeks ago

**Selected Answer: A**

Anton's misconception regarding compliance is A. The timeline for monitoring.

Anton believes that after a compliance assessment, the company should be safe for another five years, at which time he can order another check. This is fundamentally flawed. Regulatory and legislative landscapes change rapidly. Compliance monitoring is an ongoing process, not a one-time event

upvoted 1 times

**Dhruval** 7 months, 2 weeks ago

**Selected Answer: A**

compliance need to be continuously demonstrated. Even if an organization comply/certify to standards like ISO27701, every year surveillance audit by external auditors happen to evaluate org.'s compliance and basis outcome of audit org.'s certificate is renewed or otherwise.

upvoted 1 times

**Rocketly** 11 months, 2 weeks ago

**Selected Answer: A**

A - timeline for monitoring. He believes he can check again after a gap of 5 years. However, monitoring for changes should be continuous

upvoted 1 times

**humhain** 1 year, 4 months ago

Selected Answer: A

The timeline for monitoring  
upvoted 1 times

🗨️ 👤 **katizeti** 1 year, 5 months ago

A should be correct. Regulatory and legislative changes can occur at any time, and it is crucial to monitor compliance on an ongoing basis to ensure that the company remains in compliance with applicable laws and regulations.  
upvoted 2 times

🗨️ 👤 **Cock** 1 year, 9 months ago

Selected Answer: A

Compliance with regulatory and legislative changes is an ongoing process that requires continuous monitoring and adaptation.  
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

Selected Answer: A

Should be A  
upvoted 2 times

🗨️ 👤 **DracoL** 2 years, 2 months ago

Selected Answer: B

Documentation of this analysis will show auditors due diligence. This documentation of analysis doesn't prove his company is comply to regulatory requirement. A proper audit and method of record keeping is required. A is kind of right also because compliance is not a 5 year 1 time activity.  
upvoted 3 times

🗨️ 👤 **Boerenkool** 2 years, 4 months ago

Should be A  
upvoted 4 times

🗨️ 👤 **Larryqwe** 2 years, 4 months ago

Answer should be A  
upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production – not data processing – and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.

To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth – his uncle's vice president and longtime confidante – wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password-protected system that only he and Kenneth can access.

Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.

After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.

Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check. Documentation of this analysis will show auditors due diligence.

Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

What would the company's legal team most likely recommend to Anton regarding his planned communication with customers?

- A. To send consistent communication.
- B. To shift to electronic communication.
- C. To delay communications until local authorities are informed.
- D. To consider under what circumstances communication is necessary.

**Suggested Answer:** D

Community vote distribution

D (100%)

 **Rocketly** 11 months, 2 weeks ago

**Selected Answer:** D

Agree with D - depending on the applicable legal regime, notification may not be required if the data was encrypted

upvoted 3 times

Why were the nongovernmental privacy organizations, Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC), established?

- A. To promote consumer confidence in the Internet industry.
- B. To improve the user experience during online shopping.
- C. To protect civil liberties and raise consumer awareness.
- D. To promote security on the Internet through strong encryption.

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **ShadyB** 4 months, 3 weeks ago

**Selected Answer: C**

The nongovernmental privacy organizations, Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC), were established  
C. To protect civil liberties and raise consumer awareness.

Core Mission: Both EFF and EPIC are dedicated to defending civil liberties in the digital world. Their primary focus is on protecting privacy, free speech, and other rights in the face of technological advancements and government actions.

Advocacy and Education: They engage in advocacy, litigation, and public education to raise awareness about privacy issues and promote responsible technology policies.

Here's why the other options are less accurate:

A. To promote consumer confidence in the Internet industry: While consumer confidence is a byproduct of their work, it's not their primary objective. They are focused on rights, not industry promotion.

B. To improve the user experience during online shopping: User experience is not their primary focus. They are focused on the underlying rights and protections.

upvoted 1 times

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: C**

Websites refer to civil liberties, democratic values etc

upvoted 1 times


What is the main function of the Asia-Pacific Economic Cooperation Privacy Framework?

- A. Enabling regional data transfers.
- B. Protecting data from parties outside the region.
- C. Establishing legal requirements for privacy protection in the region.
- D. Marketing privacy protection technologies developed in the region.

**Suggested Answer: A**

*Community vote distribution*



A (100%)

  **humhain** 10 months, 3 weeks ago

**Selected Answer: A**

<https://iapp.org/resources/article/apec-privacy-framework/>

upvoted 2 times

  **emily0922** 1 year, 5 months ago



A is correct

upvoted 3 times

  **giomike** 1 year, 8 months ago

Overall, the function of the APEC Privacy Framework is to promote the protection of personal information while facilitating cross-border trade and commerce in the Asia-Pacific region, and to encourage cooperation and capacity building among APEC member economies in the area of privacy protection.

upvoted 2 times

  **giomike** 1 year, 7 months ago

Overall, the main function of the APEC Privacy Framework is to promote privacy protection, encourage cross-border data flows, and establish a common understanding among APEC member economies on privacy principles and practices.

upvoted 2 times

  **mansour975** 1 year, 8 months ago

C maybe correct

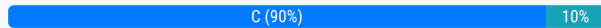
upvoted 4 times

Which of the following is TRUE about the Data Protection Impact Assessment (DPIA) process as required under the General Data Protection Regulation (GDPR)?

- A. The DPIA result must be reported to the corresponding supervisory authority.
- B. The DPIA report must be published to demonstrate the transparency of the data processing.
- C. The DPIA must include a description of the proposed processing operation and its purpose.
- D. The DPIA is required if the processing activity entails risk to the rights and freedoms of an EU individual.

**Suggested Answer: C**

Community vote distribution



🗳️ 👤 **DenZ\_101** 1 month, 4 weeks ago

**Selected Answer: D**

"A DPIA is required if the processing is likely to result in a high risk to the rights and freedoms of natural persons."  
(Chapter 4: Assess – Data Protection Impact Assessments)

Also see: GDPR Article 35

upvoted 1 times

🗳️ 👤 **Dhrumal** 7 months, 2 weeks ago

**Selected Answer: C**

risk severity or magnitude is not mentioned hence omitted option D.

upvoted 1 times

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: C**

Cannot be D as the threshold is 'high' risk and not just any risk. C describes a couple of basic elements required within a DPIA

upvoted 3 times

🗳️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: C**

DPIA only required for high risk

upvoted 1 times

🗳️ 👤 **xBrowseRx** 1 year, 1 month ago

**Selected Answer: C**

C. The DPIA must include a description of the proposed processing operation and its purpose.

The GDPR requires that a DPIA contain "a systematic description of the envisaged processing operations and the purposes of the processing" as one of its key elements. This is clearly stated in Article 35 of the GDPR which outlines the requirements for conducting a DPIA.

For D, The DPIA is specifically required when the data processing is "likely to result in a high risk to the rights and freedoms of natural persons", not just if there is any risk involved.

upvoted 4 times

As a Data Protection Officer (DPO), one of your roles entails monitoring changes in laws and regulations and updating policies accordingly. How would you most effectively execute this responsibility?

- A. Consult an external lawyer.
- B. Regularly engage regulators.
- C. Attend workshops and interact with other professionals.
- D. Subscribe to email list-serves that report on regulatory changes.

**Suggested Answer: D**

Community vote distribution



🗳️ 👤 **DenZ\_101** 1 month, 4 weeks ago

**Selected Answer: B**

"Privacy professionals must remain informed of legal developments through regulatory bulletins, direct contact with regulators, industry associations, and continuous learning."

(Chapter 3: Laws and Regulations; paraphrased)

upvoted 1 times

🗳️ 👤 **44d06fe** 3 months, 3 weeks ago

**Selected Answer: D**

D was referred to by the textbook

upvoted 1 times

🗳️ 👤 **ShadyB** 4 months, 3 weeks ago

**Selected Answer: C**

C. Attend workshops and interact with other professionals.

Comprehensive Learning: Workshops and professional interactions provide a platform for in-depth understanding of complex regulatory changes, best practices, and practical applications.

Networking and Collaboration: Interacting with other professionals allows for the exchange of knowledge, experiences, and insights, which can be invaluable in staying up-to-date.

Expert Insights: Workshops often feature experts in the field who can provide valuable guidance and answer specific questions.

Here's why D is less comprehensive:

D. Subscribe to email list-serves: Email list-serves are a good source of information, but they may not provide the same level of in-depth understanding and practical application as workshops and professional interactions. They are a good supplement to other methods.

upvoted 1 times

🗳️ 👤 **Drackos2** 6 months, 3 weeks ago

**Selected Answer: D**

Subscribe to email newsletter is the best approach to stay current.

upvoted 2 times

🗳️ 👤 **7f814c6** 11 months ago

**Selected Answer: C**

Attending workshops and interacting with other professionals allows you to stay current with the latest trends and changes in the regulatory landscape. It also provides opportunities to discuss practical implications, share experiences, and learn from peers in the field. This approach helps ensure that you are not only informed about regulatory changes but also understand their impact on data protection practices and policies.

While consulting an external lawyer (A) and subscribing to email list-serves (D) are valuable resources, and regularly engaging with regulators (B) is important for compliance, the interactive and comprehensive nature of workshops and professional networking often provides a more holistic understanding of regulatory developments.

upvoted 1 times

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: D**

Email lists is the answer referred to in the textbook, and is the more systematic approach. C would also be useful

upvoted 3 times

🔖 👤 **xBowseRx** 1 year, 1 month ago

**Selected Answer: C**

C.

As a Data Protection Officer (DPO), attending workshops and interacting with other data privacy professionals is the most effective way to stay updated on changes in laws and regulations and ensure your organization's policies remain compliant.

Email lists are great but emails can get lost or marked as spam, whereas a big change in a regulation will likely be brought up amongst professionals in the same field.

upvoted 2 times



## SCENARIO -

Please use the following to answer the next question:

John is the new privacy officer at the prestigious international law firm – A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe. During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor – MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

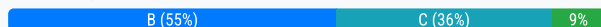
At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.

Which of the following is the most effective control to enforce MessageSafe's implementation of appropriate technical countermeasures to protect the personal data received from A&M LLP?

- A. MessageSafe must apply due diligence before trusting Cloud Inc. with the personal data received from A&M LLP.
- B. MessageSafe must flow-down its data protection contract terms with A&M LLP to Cloud Inc.
- C. MessageSafe must apply appropriate security controls on the cloud infrastructure.
- D. MessageSafe must notify A&M LLP of a data breach.

**Suggested Answer: B**

*Community vote distribution*



**DenZ\_101** 1 month, 4 weeks ago

**Selected Answer: B**

"Where personal data is shared with a vendor that uses subprocessors, privacy obligations and standards must be flowed down contractually to the subprocessor."

(Chapter 5: Protect – Third-Party Contracts)

upvoted 1 times

**Rocketly** 11 months, 2 weeks ago

**Selected Answer: B**

The question is not about security measures themselves, but how best to 'enforce' security measures in this relationship. This is always via the data processing contract terms, which need to flow down through subcontractors

upvoted 1 times

**Habeeb007** 1 year ago

C - The questions is about technical countermeasures and not administrative or physical controls

upvoted 1 times

**thecheaterz** 1 year, 1 month ago

**Selected Answer: B**

Message safe needs to flow down its obligations to the sub processor

upvoted 2 times

**MaritzTee** 1 year, 1 month ago

**Selected Answer: C**

This option directly addresses the need for MessageSafe to implement and maintain technical security measures on the cloud infrastructure. Given that the previous breach was due to a technical error, focusing on robust security controls is crucial to prevent similar incidents.

upvoted 4 times

🗨️ 👤 **DPRamone** 1 year, 4 months ago

**Selected Answer: B**

Cloud Inc. needs to comply with the same requirements MessageSafe has in its contract with the controller.

upvoted 2 times

🗨️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: D**

MessageSafe must notify A&M LLP of a data breach.

upvoted 1 times

🗨️ 👤 **katizeti** 1 year, 5 months ago

I would say C

upvoted 3 times

🗨️ 👤 **baranikumar\_v** 1 year, 11 months ago

B. Requirement shall flow from A to B. Then B shall ensure that the contractor/partner C abides to the same requirements.

upvoted 2 times

🗨️ 👤 **\_sleepless770** 2 years ago

B is the correct answer. The sub-processor must be held to the same standards and instructions as the processor which is MessageSafe

upvoted 2 times

🗨️ 👤 **szopenowa** 2 years, 1 month ago

maybe C?

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

John is the new privacy officer at the prestigious international law firm – A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe. During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor – MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

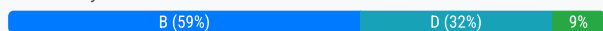
At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off- premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.

Which of the following is a TRUE statement about the relationship among the organizations?

- A. Cloud Inc. must notify A&M LLP of a data breach immediately.
- B. MessageSafe is liable if Cloud Inc. fails to protect data from A&M LLP.
- C. Cloud Inc. should enter into a data processor agreement with A&M LLP.
- D. A&M LLP's service contract must be amended to list Cloud Inc. as a sub-processor.

## Suggested Answer: B

Community vote distribution



**MaritzTee** Highly Voted 1 year, 1 month ago

**Selected Answer: B**

MessageSafe is the direct vendor to A&M LLP and is responsible for the subcontractors it engages. If Cloud Inc. fails to protect A&M LLP's data, MessageSafe, as the data processor, is liable to A&M LLP. This aligns with standard data protection regulations where the primary processor retains responsibility for the actions of its sub-processors.

upvoted 6 times

**DenZ\_101** Most Recent 1 month, 4 weeks ago

**Selected Answer: D**

"Where processors engage subprocessors, the identity of these subprocessors should be disclosed to the controller, and they should be included or referenced in the data processing agreement."

(Chapter 5 – Protect: Third-Party Contracts)

upvoted 1 times

**8bdc4dc** 4 months, 2 weeks ago

**Selected Answer: B**

A&M LLP does not need a direct DPA with Cloud Inc., but MessageSafe must have one with Cloud Inc. Since MessageSafe is A&M LLP's direct processor, MessageSafe is fully liable if Cloud Inc. fails to protect the data.

upvoted 1 times

**ShadyB** 4 months, 3 weeks ago

**Selected Answer: D**

The TRUE statement about the relationship among the organizations is D. A&M LLP's service contract must be amended to list Cloud Inc. as a sub-processor.

Sub-processing: Cloud Inc. is a sub-processor because it is processing data on behalf of MessageSafe, which is, in turn, processing data on behalf of A&M LLP. Under GDPR (Art. 28) and other similar regulations, it's essential to have clear contractual agreements that outline the responsibilities of

each party in the data processing chain. Listing Cloud Inc. as a sub-processor in the contract between A&M LLP and MessageSafe (which would require an amendment) ensures that A&M LLP has visibility and control over who is handling its data.

<https://gdpr-info.eu/art-28-gdpr/>

upvoted 1 times

🗳️ 👤 **0ef35ef** 5 months, 3 weeks ago

**Selected Answer: D**

The correct answer is D, because the GDPR and other data protection regulations require that organizations (like A&M LLP) be made aware of and have agreements in place for any sub-processors involved in the processing of personal data. Therefore, A&M LLP's service contract with MessageSafe must be amended to list Cloud Inc. as a sub-processor.

upvoted 1 times

🗳️ 👤 **9385ae2** 5 months, 3 weeks ago

**Selected Answer: B**

B.

<https://gdpr-info.eu/art-28-gdpr/>

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. 2Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

upvoted 1 times

🗳️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: B**

without information on jurisdictions we can exclude D

upvoted 2 times

🗳️ 👤 **Habeeb007** 1 year ago

The questions has references to US & EU therefore D is the correct answer

upvoted 2 times

🗳️ 👤 **BevMe** 1 year, 1 month ago

**Selected Answer: D**

When a data processor (MessageSafe) engages another party (Cloud Inc.) to process data on behalf of the data controller (A&M LLP), GDPR requires that the sub-processing be approved by the data controller. This typically involves amending the service contract to explicitly list the sub-processor

upvoted 2 times

🗳️ 👤 **MaritzTee** 1 year, 1 month ago

**Selected Answer: D**

D. A&M LLP's service contract must be amended to list Cloud Inc. as a sub-processor.

This is because Cloud Inc., as the provider of the cloud infrastructure that MessageSafe uses to host the email continuity service, is effectively acting as a sub-processor of A&M LLP's data. To comply with data protection regulations, such as the GDPR, it is important to have clear contractual agreements that identify all parties involved in the processing of personal data, including sub-processors. The contract should outline the responsibilities and obligations of each party to ensure data protection and compliance.

upvoted 2 times

🗳️ 👤 **DPRamone** 1 year, 4 months ago

**Selected Answer: B**

Under the GDPR, a sub-processor will remain liable to the processor for its own data processing operations. Ref. <https://incorporated.zone/sub-processor-compliance-obligations-under-gdpr/>

upvoted 2 times

🗳️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: A**

Cloud Inc. must notify A&M LLP of a data breach immediately.

upvoted 2 times

🗳️ 👤 **katizeti** 1 year, 5 months ago

C maybe??

upvoted 1 times

🗨️ 👤 **katizeti** 1 year, 4 months ago

D. A&M LLP's service contract must be amended to list Cloud Inc. as a sub-processor.

This option accurately reflects the data processing flow and legal obligations within the scenario.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: B**

Should be B

upvoted 1 times

🗨️ 👤 **baranikumar\_v** 1 year, 11 months ago

B may be the right answer.

upvoted 3 times

🗨️ 👤 **Alex951** 2 years ago

I suggest B

upvoted 3 times

🗨️ 👤 **szopenowa** 2 years, 1 month ago

maybe B?

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

John is the new privacy officer at the prestigious international law firm – A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe. During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor – MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off- premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.

Which of the following is NOT an obligation of MessageSafe as the email continuity service provider for A&M LLP?

- A. Privacy compliance.
- B. Security commitment.
- C. Certifications to relevant frameworks.
- D. Data breach notification to A&M LLP.

**Suggested Answer:** C

🗨️ 👤 **lulu9629** 1 year ago

C is the correct answer

upvoted 1 times

In privacy protection, what is a "covered entity"?

- A. Personal data collected by a privacy organization.
- B. An organization subject to the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA).
- C. A privacy office or team fully responsible for protecting personal information.
- D. Hidden gaps in privacy protection that may go unnoticed without expert analysis.

**Suggested Answer:** B

*Community vote distribution*

B (100%)

 **Fyssy** 2 months, 3 weeks ago

**Selected Answer: B**

organizations that must comply to HIPAA are referred to as covered entities

upvoted 1 times

Which of the following best describes proper compliance for an international organization using Binding Corporate Rules (BCRs) as a controller or processor?

- A. Employees must sign an ad hoc contractual agreement each time personal data is exported.
- B. All employees are subject to the rules in their entirety, regardless of where the work is taking place.
- C. All employees must follow the privacy regulations of the jurisdictions where the current scope of their work is established.
- D. Employees who control personal data must complete a rigorous certification procedure, as they are exempt from legal enforcement.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ **DenZ\_101** 1 month, 4 weeks ago

**Selected Answer: B**

"BCRs are legally binding internal rules adopted by multinational groups of companies to allow transfers of personal data within the same corporate group to entities located outside the EU. All employees must adhere to them, regardless of their work location."

(Chapter 3 – Applicable Privacy Laws and Regulations)

upvoted 1 times

🗳️ **humhain** 10 months, 3 weeks ago

**Selected Answer: B**

BCRs must ensure that all employees who process personal data follow the privacy regulations of the jurisdictions where the data originates from, regardless of where they are located or where the data is transferred to.

<https://www.lexology.com/library/detail.aspx?g=80239951-01b8-409f-9019-953f5233852e>

upvoted 2 times

🗳️ **Viphit** 1 year ago

Answer B: BCR are are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

upvoted 3 times

🗳️ **DracoL** 1 year, 8 months ago

**Selected Answer: B**

From a paper from PwC. The above principles need to be binding within the corporate group, as against employees and subcontractors. The documents likely to achieve this are:

- A resolution of the parent company's board to make the principles binding;
- An employee notice requiring application of the principles;
- Pro forma contract terms for use with subcontractors; and
- Intra-group contract that confers third party rights.

upvoted 3 times

🗳️ **Rita1234** 1 year, 9 months ago

Shouldn't be B?

upvoted 3 times



## SCENARIO -

Please use the following to answer the next question:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.

Immediately upon arrival, Richard was amazed at the amount of work that needed to be done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place. Richard is also concerned with the overuse of the communal copier/printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end. Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary. Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

Richard believes that a transition from the use of fax machine to Internet faxing provides all of the following security benefits EXCEPT?

- A. Greater accessibility to the faxes at an off-site location.
- B. The ability to encrypt the transmitted faxes through a secure server.
- C. Reduction of the risk of data being seen or copied by unauthorized personnel.
- D. The ability to store faxes electronically, either on the user's PC or a password-protected network server.

**Suggested Answer: A**

Community vote distribution

A (100%)

 **MaritzTee** 7 months, 3 weeks ago

**Selected Answer: A**

A. Greater accessibility to the faxes at an off-site location.


While greater accessibility to faxes at an off-site location can be seen as a benefit in terms of convenience and business continuity, it is not necessarily a security benefit. In fact, increased accessibility can sometimes introduce new security risks if not properly managed, as it may make sensitive data more vulnerable to unauthorized access. The other options (B, C, and D) directly address improvements in security, such as encryption, reducing unauthorized viewing or copying, and secure electronic storage.

upvoted 1 times

 **DPRamone** 10 months, 1 week ago

Solutions like eFax or sFax provide encryption options. Greater availability of the faxes at other locations doesn't necessarily increase security. So the answer is A.

upvoted 3 times

 **katizeti** 11 months, 3 weeks ago

Nope. A is correct

upvoted 3 times

 **lulu9629** 1 year ago

A

other options (B, C, and D) are generally security benefits associated with Internet faxing.

upvoted 3 times

 **ET1857** 1 year, 4 months ago

Correct B: The ability to encrypt the transmitted faxes through a secure server.

A is wrong because we can access the internet fax from locations outside the office ie off-site.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.

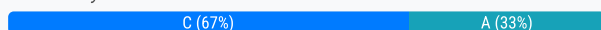
Immediately upon arrival, Richard was amazed at the amount of work that needed to be done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place. Richard is also concerned with the overuse of the communal copier/printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end. Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary. Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

As Richard begins to research more about Data Lifecycle Management (DLM), he discovers that the law office can lower the risk of a data breach by doing what?

- A. Prioritizing the data by order of importance.
- B. Minimizing the time it takes to retrieve the sensitive data.
- C. Reducing the volume and the type of data that is stored in its system.
- D. Increasing the number of experienced staff to code and categorize the incoming data.

**Suggested Answer: C**

*Community vote distribution*



**ShadyB** 4 months, 3 weeks ago

**Selected Answer: C**

The law office can lower the risk of a data breach by C. Reducing the volume and the type of data that is stored in its system.

This principle is known as data minimization. Reduced Attack Surface: The less data that's stored, the less there is to be stolen or compromised in a breach.

Reduced Risk of Accidental Disclosure: Fewer documents and files mean a lower chance of accidental loss or unauthorized access.

Easier Management: A smaller data footprint is easier to manage and secure.

Here's why the other options are less directly related to reducing breach risk:

- A. Prioritizing the data by order of importance: While prioritization is useful for incident response, it doesn't reduce the overall amount of data at risk.
  - B. Minimizing the time it takes to retrieve the sensitive data: Quick retrieval doesn't address the inherent risk of storing the data in the first place.
- upvoted 1 times

**0ef35ef** 5 months, 3 weeks ago

**Selected Answer: C**

By reducing the volume and type of data stored (Option C), Richard can significantly lower the potential for a data breach. This approach aligns directly with best practices in Data Lifecycle Management and data security by ensuring that only necessary and secure data is stored, minimizing the risk of exposure or theft.



upvoted 1 times

**Maherukh** 6 months, 2 weeks ago

**Selected Answer: A**

Prioritizing the importance of data also means categorizing, how can one reduce before knowing what he or she is deleting.

upvoted 1 times

  **ET1857** 10 months, 3 weeks ago

C is correct - key is type of data means the data is categorized and unwanted data is purged or destroyed

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.

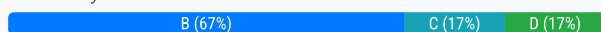
Immediately upon arrival, Richard was amazed at the amount of work that needed to be done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place. Richard is also concerned with the overuse of the communal copier/printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end. Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary. Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

Which of the following policy statements needs additional instructions in order to further protect the personal data of their clients?

- A. All faxes sent from the office must be documented and the phone number used must be double checked to ensure a safe arrival.
- B. All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily.
- C. Before any copiers, printers, or fax machines are replaced or resold, the hard drives of these devices must be deleted before leaving the office.
- D. When sending a print job containing personal data, the user must not leave the information visible on the computer screen following the print command and must retrieve the printed document immediately.

**Suggested Answer: B**

Community vote distribution



🗳️ 👤 **9385ae2** 5 months, 3 weeks ago

**Selected Answer: C**

C. Specific steps on how to do this are needed to do properly.  
upvoted 1 times

🗳️ 👤 **Vinz\_** 7 months ago

**Selected Answer: D**

The policy statement is missing the additional condition that the computer screen must be locked, otherwise information can be retrieved by anyone at the computer.  
upvoted 1 times

🗳️ 👤 **Rocketly** 11 months, 2 weeks ago

**Selected Answer: B**

Need to add info on what happens when the bin is emptied - are they stored securely then shredded?  
upvoted 1 times

🗳️ 👤 **yzx666xming** 1 year ago

c  
B is not a proper way  
upvoted 1 times

🗳️ 👤 **Boboshooter** 1 year, 1 month ago

C  
While the policy statement acknowledges the importance of wiping hard drives before disposal, it lacks specific instructions on how to perform this

task effectively. To enhance data security, Richard should provide detailed steps for securely erasing data from these devices, including any necessary software tools or procedures. This ensures that sensitive information does not remain accessible after the equipment leaves the office.

upvoted 3 times

🗨️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: B**

This policy statement is insufficient because it does not specify how the unused copies, prints, and faxes should be discarded. Simply throwing them into a recycling bin may expose them to unauthorized access or theft by anyone who has access to the bin or its contents. Also, emptying the bin daily may not be frequent enough to prevent accumulation or overflow of sensitive documents.

upvoted 3 times

🗨️ 👤 **Gh789** 1 year, 10 months ago

B. If it contains PI, the paper should be shredded

upvoted 3 times

🗨️ 👤 **ET1857** 1 year, 10 months ago

B. All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily.

Additional information : what to do if the unused paper contains PII. Should we re-use it or destroy it ?

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.

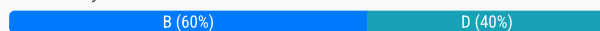
Immediately upon arrival, Richard was amazed at the amount of work that needed to be done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place. Richard is also concerned with the overuse of the communal copier/printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end. Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary. Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.

Richard needs to closely monitor the vendor in charge of creating the firm's database mainly because of what?

- A. The vendor will be required to report any privacy violations to the appropriate authorities.
- B. The vendor may not be aware of the privacy implications involved in the project.
- C. The vendor may not be forthcoming about the vulnerabilities of the database.
- D. The vendor will be in direct contact with all of the law firm's personal data.

## Suggested Answer: B

Community vote distribution



🗳️ **Vinz\_** 7 months ago

**Selected Answer: B**

B is correct, while D is incorrect because the company is in charge of "creating the database", not necessarily maintaining it.  
upvoted 1 times

🗳️ **Boboshooter** 7 months, 1 week ago

D, should be correct  
upvoted 2 times

🗳️ **Stevenciu** 9 months, 1 week ago

**Selected Answer: D**

I think Richard should adopt a Trust but Verify stance.  
upvoted 2 times

🗳️ **DPRamone** 10 months ago

**Selected Answer: B**

Privacy by design needs to be incorporated into the DB development project. C sounds less logical because the DB hasn't been created yet.  
upvoted 2 times

🗳️ **katizeti** 11 months, 3 weeks ago

C. The vendor may not be forthcoming about the vulnerabilities of the database  
upvoted 1 times

🗳️ **Gh789** 1 year, 5 months ago

C : with the onboarding of the vendor, DPA would be signed which will provide insights into personal data handling  
upvoted 1 times



What should be the first major goal of a company developing a new privacy program?

- A. To survey potential funding sources for privacy team resources.
- B. To schedule conversations with executives of affected departments.
- C. To identify potential third-party processors of the organization's information.
- D. To create Data Lifecycle Management policies and procedures to limit data collection.

**Suggested Answer: B**

Community vote distribution

B (100%)

  **emily0922** Highly Voted 1 year, 5 months ago

B? To get to know the needs of the various stakeholders first  
upvoted 6 times

  **ShadyB** Most Recent 4 months, 3 weeks ago

**Selected Answer: B**

The first major goal should be B.

Executive Buy-in and Collaboration: Establishing a successful privacy program requires support and cooperation across the entire organization.

Conversations with executives of affected departments are crucial for:

- 1- Gaining their understanding of the importance of privacy.
- 2- Identifying existing data processing activities and potential risks.
- 3- Securing their commitment to implementing privacy measures.
- 4- Establishing cross-departmental collaboration.

Understanding the Organization: Before any policies or procedures can be developed, the privacy team must understand the organization's data flows, business processes, and existing practices.

Here's why the other options are less crucial as a first step:

- C. it comes after understanding the organization's internal data processing activities.
- D. Developing policies and procedures is a later step.

upvoted 1 times

  **Boboshooter** 7 months, 1 week ago

D should be correct  
upvoted 1 times

  **BevMe** 7 months, 2 weeks ago

**Selected Answer: B**

Necessary to build support and alignment with the stakeholders.

upvoted 2 times

  **Stevenciu** 9 months, 1 week ago

**Selected Answer: B**

I think the first thing to do is to secure buy-in from key stakeholders across the organization.

upvoted 2 times

  **giomike** 11 months, 2 weeks ago

The first major goal of a company developing a new privacy program should be to establish a comprehensive understanding of privacy requirements, risks, and regulations relevant to its operations. This involves conducting a thorough privacy assessment to identify and assess the personal data the company collects, processes, and stores.

upvoted 1 times

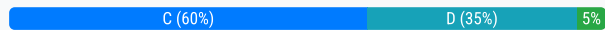


Which is TRUE about the scope and authority of data protection oversight authorities?

- A. The Office of the Privacy Commissioner (OPC) of Canada has the right to impose financial sanctions on violators.
- B. All authority in the European Union rests with the Data Protection Commission (DPC).
- C. No one agency officially oversees the enforcement of privacy regulations in the United States.
- D. The Asia-Pacific Economic Cooperation (APEC) Privacy Frameworks require all member nations to designate a national data protection authority.

**Suggested Answer: C**

Community vote distribution



**Stevenciu** Highly Voted 1 year, 3 months ago

**Selected Answer: C**

In the United States, there is no single federal-level data protection oversight authority equivalent to what exists in many other jurisdictions.  
upvoted 5 times

**DenZ\_101** Most Recent 1 month, 4 weeks ago

**Selected Answer: C**

U.S. = fragmented, EU = federated, Canada = independent but limited enforcement, APEC = voluntary coordination.  
upvoted 1 times

**44d06fe** 3 months, 3 weeks ago

**Selected Answer: D**

From APEC:

37. There are several options for giving effect to the Framework and securing privacy protections for individuals including legislative, administrative, industry selfregulatory or a combination of these policy instruments. In practice, the Framework

7

See clauses 43-45 below.

APEC Privacy Framework 2015

Page 24 of 31

is meant to be implemented in a flexible manner that can accommodate various models of enforcement, including through Privacy Enforcement Authorities, multiagency enforcement bodies, a network of designated industry bodies, courts and tribunals, or a combination of the above, as member economies deem appropriate.

upvoted 1 times

**Ashwin123** 5 months, 3 weeks ago

**Selected Answer: C**

C is not the answer because - The APEC Privacy Framework set in motion the process of creating the APEC Cross-Border Privacy Rules system. The CBPR system has now been formally joined by the United States, Canada, Japan and Mexico, with more nations soon to follow. The CBPR program is analogous to the EU-U.S. Privacy Shield in that they both provide a means for self-assessment, compliance review, recognition/acceptance and dispute resolution/enforcement. Both systems require the designation by each country of a data protection authority (the U.S. enforcement authority is the Federal Trade Commission).

Source - <https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules>

upvoted 1 times

**Dhrumal** 7 months, 1 week ago

**Selected Answer: C**

APAC privacy framework does not mandate national data protection authority by each member country.

upvoted 1 times

**yzx666xming** 1 year ago

C

D not correct apec suggest not require  
upvoted 1 times

🗨️ **thecheaterz** 1 year, 1 month ago

**Selected Answer: C**

There is no federal privacy law in the US and hence no central enforcement  
upvoted 3 times

🗨️ **gilmofer** 1 year, 3 months ago

**Selected Answer: D**

APEC Principle 43 says the following: Member Economies should designate and make known to the other Member Economies the public authorities within their own jurisdictions that will be responsible for facilitating cross-border cooperation and information sharing between economies in connection with privacy protection.  
upvoted 1 times

🗨️ **DPRamone** 1 year, 4 months ago

**Selected Answer: D**

See <https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/> : "Both systems require the designation by each country of a data protection authority (the U.S. enforcement authority is the Federal Trade Commission)."  
upvoted 2 times

🗨️ **humhain** 1 year, 4 months ago

**Selected Answer: A**

Reference: [https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\\_index/201617/ar\\_201617/](https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/)  
upvoted 1 times

🗨️ **[Removed]** 1 year, 10 months ago

**Selected Answer: C**

C is the answer  
upvoted 1 times

🗨️ **Gh789** 1 year, 10 months ago

C - OPC does not have authority to impose fines  
upvoted 2 times

🗨️ **emily0922** 1 year, 11 months ago

C is the answer  
upvoted 2 times

🗨️ **mgmferreira** 2 years, 1 month ago

Letra C: Nos Estados Unidos, a privacidade e a proteção de dados são regulamentadas por uma combinação de leis federais e estaduais, e são supervisionadas por várias agências, dependendo do setor e do tipo de dados. No entanto, ao contrário de muitos outros países, os Estados Unidos não têm uma única agência ou autoridade central de supervisão de privacidade.  
upvoted 3 times

🗨️ **Boerenkool** 2 years, 3 months ago

**Selected Answer: D**

should be D  
upvoted 3 times

What should a privacy professional keep in mind when selecting which metrics to collect?

- A. Metrics should be reported to the public.
- B. The number of metrics should be limited at first.
- C. Metrics should reveal strategies for increasing company earnings.
- D. A variety of metrics should be collected before determining their specific functions.

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **humhain** Highly Voted 10 months, 3 weeks ago

**Selected Answer: B**

Metrics are quantitative measures that help evaluate the performance and effectiveness of a privacy program. However, collecting too many metrics can be overwhelming, confusing, and costly. Therefore, a privacy professional should start with a few key metrics that are relevant, meaningful, actionable, and aligned with the organization's privacy goals and priorities.

upvoted 6 times

🗳️ 👤 **DenZ\_101** Most Recent 1 month, 4 weeks ago

**Selected Answer: B**

"Start with a limited number of well-defined, meaningful metrics that align with program goals. Avoid overwhelming the process early on."  
(Chapter 7 – Program Performance & Metrics)

upvoted 1 times

🗳️ 👤 **Viphit** 1 year ago

B should be correct answers

upvoted 1 times

🗳️ 👤 **emily0922** 1 year, 4 months ago

B, too many metrics is not good, it should focus on the business objectives

upvoted 2 times

🗳️ 👤 **DracoL** 1 year, 8 months ago

**Selected Answer: B**

B is the correct answer. Cannot be A

upvoted 2 times

🗳️ 👤 **Luton** 1 year, 8 months ago

Should be B

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

What Data Lifecycle Management (DLM) principle should the company follow if they end up allowing departments to interpret the privacy policy differently?

- A. Prove the authenticity of the company's records.
- B. Arrange for official credentials for staff members.
- C. Adequately document reasons for inconsistencies.
- D. Create categories to reflect degrees of data importance.

**Suggested Answer: C**

*Community vote distribution*

C (100%)


 **DenZ\_101** 1 month, 4 weeks ago

**Selected Answer: C**

"To support accountability, organizations must document how decisions are made, especially when there is variation in how privacy rules are interpreted or applied."

(Chapter 4: Data Lifecycle Management – Governance and Risk)

upvoted 1 times

 **ShadyB** 4 months, 3 weeks ago

**Selected Answer: C**

The Data Lifecycle Management (DLM) principle that the company should follow if they allow departments to interpret the privacy policy differently is C. Adequately document reasons for inconsistencies.

Accountability and Auditability: If departments are allowed to deviate from a central policy, there must be a clear record of why those deviations occurred. This documentation is essential for accountability, auditing, and demonstrating compliance.

Risk Mitigation: By documenting inconsistencies, the company can track and manage the potential risks associated with these variations. It allows them to identify patterns, address potential problems, and make informed decisions about policy adjustments.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

What is the most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is NOT adequate?

- A. The company needs to have policies and procedures in place to guide the purchasing decisions.
- B. The privacy notice for customers and the Business Continuity Plan (BCP) still need to be reviewed.
- C. Staff members across departments need time to review technical information concerning any new databases.
- D. Senior staff members need to first commit to adopting a minimum number of Privacy Enhancing Technologies (PETs).

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **ShadyB** 4 months, 3 weeks ago

**Selected Answer: A**

The most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is NOT adequate is A. The company needs to have policies and procedures in place to guide the purchasing decisions.

- Foundation for Technology: Before purchasing any equipment, it's crucial to have a solid framework of policies and procedures. These policies will dictate:

- 1- What types of data are being stored.
- 2- How that data should be protected.
- 3- Who has access to the data.
- 4- How data is disposed of.

- Preventing Ad Hoc Purchases: Without policies, equipment purchases might be made in an ad hoc manner, leading to inconsistencies, vulnerabilities, and potential compliance issues.

Here's why the B is less likely to be the primary concern:

B. The privacy notice for customers and the Business Continuity Plan (BCP) still need to be reviewed: While important, these are not the immediate prerequisites for deciding on IT equipment. Policies and procedures are more fundamental.

upvoted 1 times



## SCENARIO -

Please use the following to answer the next question:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

If Amira and Sadie's ideas about adherence to the company's privacy policy go unchecked, the Federal Communications Commission (FCC) could potentially take action against NatGen for what?

- A. Deceptive practices.
- B. Failing to institute the hotline.
- C. Failure to notify of processing.
- D. Negligence in consistent training.

**Suggested Answer: A**

*Community vote distribution*

C (50%)


A (50%)

 **kuansong** 5 months, 2 weeks ago

**Selected Answer: C**

All members could access and handle complaints, which is beyond customer expectations.

upvoted 1 times

 **Dhruval** 7 months, 1 week ago

**Selected Answer: A**

allowing all members to handle complaints means violation of 'need-to-know' principle and 'principle of least privilege'.

upvoted 1 times



## SCENARIO -

Please use the following to answer the next question:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.

Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.

Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.

Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.

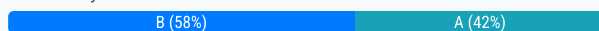
Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.

Based on the scenario, what additional change will increase the effectiveness of the privacy compliance hotline?

- A. Outsourcing the hotline.
- B. A system for staff education.
- C. Strict communication channels.
- D. An ethics complaint department.

**Suggested Answer: B**

*Community vote distribution*



**ShadyB** 4 months, 3 weeks ago

**Selected Answer: B**

The additional change that will increase the effectiveness of the privacy compliance hotline is B. A system for staff education.

Here's why:

- Proper Training is Essential: Employees taking turns handling hotline reports need to be trained on: 1) Privacy laws and regulations. 2) The company's privacy policies. 3) How to identify and document privacy violations. 4) How to handle sensitive information.

How to escalate issues appropriately.

- Without proper training, employees will lack the knowledge and skills to effectively handle hotline reports, leading to inconsistent and potentially harmful outcomes.

Here's why A is less crucial in this specific scenario:

A. Outsourcing the hotline: While outsourcing can bring expertise, it doesn't address the fundamental issue of untrained personnel. Even outsourced staff need clear guidelines and company-specific knowledge.

upvoted 2 times

**9385ae2** 5 months, 3 weeks ago

**Selected Answer: A**

Answer A will provide confidentiality as opposed to another email learning about what another employee is complaining about. This should grow trust and transparency, not reduce it.

upvoted 1 times

🗨️ 👤 **KennyDo** 8 months ago

**Selected Answer: B**

It should be B. While outsourcing the hotline may provide a level of professionalism, it could reduce trust and transparency among employees, as they may feel uncomfortable discussing sensitive privacy concerns with a third-party provider.

upvoted 1 times

🗨️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: B**

You must train staff to teach them how to use the hotline appropriately.

upvoted 2 times

🗨️ 👤 **MaritzTee** 1 year, 1 month ago

**Selected Answer: B**

Educating staff about privacy laws, company privacy policies, and the importance of compliance is crucial. It ensures that employees understand what constitutes a privacy policy violation and how to handle such issues appropriately. Education can empower employees to recognize and report genuine concerns effectively, which enhances the overall effectiveness of the hotline.

upvoted 2 times

🗨️ 👤 **katizeti** 1 year, 5 months ago

Not A. In my opinion B is correct. To ensure that employees are aware of the hotline and how to use it, NatGen could consider implementing a system for staff education.

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: A**

Should be A

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: A**

A. Outsourcing the hotline.

Outsourcing ensures that the hotline is managed by individuals trained in privacy and compliance, making it more effective in addressing and documenting any concerns or violations reported by callers.

upvoted 3 times

If an organization maintains a separate ethics office, to whom would its officer typically report to in order to retain the greatest degree of independence?

- A. The Board of Directors.
- B. The Chief Financial Officer (CFO).
- C. The Human Resources (HR) Director.
- D. The organization's General Counsel.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗨️ 👤 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

The Board of Directors. - This is the highest governing body in most organizations. Reporting directly to the board ensures that the ethics office remains independent from day-to-day operational pressures and potential conflicts of interest.

upvoted 3 times

What is a key feature of the privacy metric template adapted from the National Institute of Standards and Technology (NIST)?

- A. It provides suggestions about how to collect and measure data.
- B. It can be tailored to an organization's particular needs.
- C. It is updated annually to reflect changes in government policy.
- D. It is focused on organizations that do business internationally.

**Suggested Answer: B**

Community vote distribution

B (76%)

A (24%)

🗳️ 👤 **Ssourav** Highly Voted 1 year, 10 months ago

**Selected Answer: B**

NIST's frameworks and guidelines are intentionally designed to be adaptable, allowing organizations to implement them in a way that aligns with their specific risks, needs, and business environments.

upvoted 6 times

🗳️ 👤 **Ashwin123** Most Recent 5 months, 3 weeks ago

**Selected Answer: B**

A key feature of the privacy metric template adapted from the NIST Privacy Framework is its flexibility to be tailored to an organization's specific needs and allows them to identify and measure privacy risks based on their unique data practices and industry context; essentially, it provides a customizable framework for assessing and managing privacy risks across different organizations, rather than a rigid set of rules.

upvoted 2 times

🗳️ 👤 **alaaz** 7 months, 2 weeks ago

**Selected Answer: A**

The NIST privacy metric template provides a framework for organizations to measure and assess their privacy program's effectiveness. It includes a set of suggested metrics and methods for collecting and analyzing data to measure privacy program performance. The template provides guidance on how to select and apply metrics to different aspects of the privacy program, such as data security, data quality, and privacy compliance.

upvoted 1 times

🗳️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: A**

The NIST privacy metric template provides a framework for organizations to measure and assess their privacy program's effectiveness. It includes a set of suggested metrics and methods for collecting and analyzing data to measure privacy program performance. The template provides guidance on how to select and apply metrics to different aspects of the privacy program, such as data security, data quality, and privacy compliance. It also provides a structured process for developing a privacy metric program that aligns with an organization's unique goals, objectives, and requirements.

upvoted 3 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: B**

Should be B

upvoted 2 times

🗳️ 👤 **mgmferreira** 2 years, 1 month ago

**Selected Answer: B**

Deve ser B

upvoted 3 times

What United States federal law requires financial institutions to declare their personal data collection practices?

- A. The Kennedy-Hatch Disclosure Act of 1997.
- B. The Gramm-Leach-Bliley Act of 1999.
- C. SUPCLA, or the federal Superprivacy Act of 2001.
- D. The Financial Portability and Accountability Act of 2006.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

## SCENARIO -

Please use the following to answer the next question:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

What are the next action steps?

Which of the following would be most effectively used as a guide to a systems approach to implementing data protection?

- A. Data Lifecycle Management Standards.
- B. United Nations Privacy Agency Standards.
- C. International Organization for Standardization 9000 Series.
- D. International Organization for Standardization 27000 Series.

**Suggested Answer: D**

*Community vote distribution*

D (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: D**

International Organization for Standardization 27000 Series.

The ISO/IEC 27000 series, often referred to as the ISO 27000 series, provides best practices for information security management. It offers guidelines and standards for establishing, implementing, maintaining, and continually improving an information security management system. This is particularly relevant for data protection and is widely recognized and adopted by organizations around the world for this purpose.

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

What are the next action steps?

How can the company's privacy training program best be further developed?

- A. Through targeted curricula designed for specific departments.
- B. By adopting e-learning to reduce the need for instructors.
- C. By using industry standard off-the-shelf programs.
- D. Through a review of recent data breaches.

**Suggested Answer: A**

Currently there are no comments in this discussion, be the first to comment!

## SCENARIO -

Please use the following to answer the next question:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

What are the next action steps?



What stage of the privacy operational life cycle best describes the company's current privacy program?

- A. Assess.
- B. Protect.
- C. Respond.
- D. Sustain.

**Suggested Answer: D**

Community vote distribution

D (100%)

  **ShadyB** 4 months, 3 weeks ago

**Selected Answer: D**

Sustain:

- The program is established and integrated into the company's operations.
- Privacy protection is now an accepted component of all current operations.
- The focus is on maintaining and improving the program's effectiveness over time.
- The company is beyond the initial stages of assessment, protection, and response. They are now in a phase of continuous improvement.

Here's why the other options are less accurate:

A. Assess:

The company has already completed the initial assessment phase when the director was hired and began implementing the program.

B. Protect:

While protection is ongoing, the company has moved beyond simply implementing protective measures. They are now focused on maintaining and enhancing those measures.

C. Respond:

The company has not had a reportable incident in three years, indicating that they are not in a constant state of incident response.

upvoted 1 times

  **Od0ded9** 1 year ago

Definitely D. Sustain

upvoted 1 times

  **emily0922** 1 year, 11 months ago



Agree with D, "What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

What are the next action steps?" Maintaining - Audits, Awareness and Training

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

What are the next action steps?

What practice would afford the Director the most rigorous way to check on the program's compliance with laws, regulations and industry best practices?

- A. Auditing.
- B. Monitoring.
- C. Assessment.
- D. Forensics.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** Highly Voted 1 year, 10 months ago

**Selected Answer: A**

Auditing provides a systematic, independent, and documented process for obtaining evidence and evaluating it objectively to determine the extent to which criteria are fulfilled. In the context of data protection and compliance, an audit would offer the most rigorous method to ensure that the company's program meets the standards set by laws, regulations, and industry best practices.

upvoted 8 times

🗳️ 👤 **Rocketly** Most Recent 1 year ago

**Selected Answer: A**

Auditing is a more rigorous approach than monitoring

upvoted 1 times

🗳️ 👤 **0d0ded9** 1 year ago

Answer is A. Analyzing performance of the governance structure is essential to its success.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: A**


Should be A

upvoted 3 times

🗳️ 👤 **Gh789** 1 year, 10 months ago



C - Privacy Assessments measure organizations compliance with laws, regulations, adopted standards and internal policies and procedures.

upvoted 1 times

  **emily0922** 1 year, 11 months ago

I suggest A



upvoted 2 times

  **DracoL** 2 years, 2 months ago

**Selected Answer: A**

monitoring uses metrics to monitor but doesnt show if it comply. Audit is definitely the better answer

upvoted 4 times

  **Luton** 2 years, 2 months ago

Should be A

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

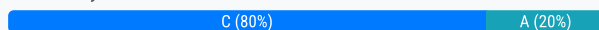
What are the next action steps?

What analytic can be used to track the financial viability of the program as it develops?

- A. Cost basis.
- B. Gap analysis.
- C. Return to investment.
- D. Breach impact modeling.

**Suggested Answer: C**

Community vote distribution



**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: C**

Return on Investment (ROI) is an analytic that can track the financial viability of a program as it develops. It measures the financial return on the resources invested in the privacy program. By calculating ROI, you can assess how well the investment in data protection is paying off in terms of reducing risks, avoiding financial penalties, and improving operational efficiency, among other factors. This allows the organization to determine whether the costs of the privacy program are justified by the benefits it provides.

Cost basis: While understanding the cost basis (the total cost of implementing the privacy program) is important, it doesn't measure the financial return or viability of the program in terms of benefits received from that investment. It's more of a starting point rather than an analytic for tracking financial viability.

upvoted 2 times

**KennyDo** 8 months ago

**Selected Answer: C**

Should be C

upvoted 2 times

**yzx666xming** 1 year ago

**Selected Answer: A**

C should be roi? To investment is wrong?

upvoted 1 times

**emily0922** 1 year, 11 months ago

C is correct

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

As the Director of data protection for Consolidated Records Corporation, you are justifiably pleased with your accomplishments so far. Your hiring was precipitated by warnings from regulatory agencies following a series of relatively minor data breaches that could easily have been worse. However, you have not had a reportable incident for the three years that you have been with the company. In fact, you consider your program a model that others in the data storage industry may note in their own program development.

You started the program at Consolidated from a jumbled mix of policies and procedures and worked toward coherence across departments and throughout operations. You were aided along the way by the program's sponsor, the vice president of operations, as well as by a Privacy Team that started from a clear understanding of the need for change.

Initially, your work was greeted with little confidence or enthusiasm by the company's "old guard" among both the executive team and frontline personnel working with data and interfacing with clients. Through the use of metrics that showed the costs not only of the breaches that had occurred, but also projections of the costs that easily could occur given the current state of operations, you soon had the leaders and key decision-makers largely on your side. Many of the other employees were more resistant, but face-to-face meetings with each department and the development of a baseline privacy training program achieved sufficient "buy-in" to begin putting the proper procedures into place.

Now, privacy protection is an accepted component of all current operations involving personal or protected data and must be part of the end product of any process of technological development. While your approach is not systematic, it is fairly effective.

You are left contemplating:

What must be done to maintain the program and develop it beyond just a data breach prevention program?

How can you build on your success?

What are the next action steps?

What process could most effectively be used to add privacy protections to a new, comprehensive program being developed at the company?

- A. Privacy by Design (PbD).
- B. Privacy Step Assessment.
- C. Information Security Planning.
- D. Innovation Privacy Standards.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Rocketly** 1 year ago

**Selected Answer: A**

New programs should always implement PbD  
upvoted 1 times

🗳️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: A**

Privacy by Design (PbD)  
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: A**

Should be A  
upvoted 2 times

🗳️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: A**



Privacy by Design (PbD) is a principle and approach that integrates privacy protections into the entire lifecycle of a system, product, or process, starting at the initial design phase.  
upvoted 3 times

🗳️ 👤 **DracoL** 2 years, 2 months ago

**Selected Answer: A**

In CIPM, Privacy by Design is key words. While Security by Design is more towards Cybersecurity side of track. PdD is always mention. So go with A

upvoted 3 times

  **Luton** 2 years, 2 months ago

Should be A

upvoted 1 times

Which of the following indicates you have developed the right privacy framework for your organization?

- A. It includes a privacy assessment of each major system.
- B. It improves the consistency of the privacy program.
- C. It works at a different type of organization.
- D. It identifies all key stakeholders by name.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ 👤 **Rocketly** 1 year ago

**Selected Answer: B**

Consistency is key to success  
upvoted 1 times

🗳️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: B**

Developing the right privacy framework for your organization means that you have a clear and coherent set of policies, procedures, and practices that align with your privacy objectives and obligations. A good privacy framework should improve the consistency of the privacy program by ensuring that all relevant stakeholders understand and follow the same standards and expectations across different functions, processes, and systems.

A consistent privacy program can also help reduce errors, risks, and costs associated with privacy compliance.

upvoted 3 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: B**

Should be B  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: B**

A good privacy framework should bring consistency across the organization, ensuring that privacy practices and policies are uniformly understood and implemented.

upvoted 3 times

🗳️ 👤 **Luton** 2 years, 2 months ago

Should be B  
upvoted 3 times



Rationalizing requirements in order to comply with the various privacy requirements required by applicable law and regulation does NOT include which of the following?

- A. Harmonizing shared obligations and privacy rights across varying legislation and/or regulators.
- B. Implementing a solution that significantly addresses shared obligations and privacy rights.
- C. Applying the strictest standard for obligations and privacy rights that doesn't violate privacy laws elsewhere.
- D. Addressing requirements that fall outside the common obligations and rights (outliers) on a case-by-case basis.

**Suggested Answer: B**

Community vote distribution



**ShadyB** 4 months, 3 weeks ago

**Selected Answer: B**

Here's why: 1) Rationalizing is About Analysis, Not Implementation: Rationalizing requirements is the process of analyzing and organizing the various obligations and rights imposed by different laws and regulations. It's a preparatory step, not the actual implementation of a solution. 2) Implementation Follows Rationalization: Implementing a solution comes after the requirements have been rationalized. The process of rationalizing determines what the solution should address.

Here's why the other options are part of rationalizing requirements:

- A. Harmonizing: This is a core part of rationalization, as it involves finding common ground among different requirements.
- C. Applying the strictest standard: This is a common strategy in rationalization, as it ensures compliance with the most stringent requirements.
- D. Addressing requirements that fall outside the common obligations: This is also a part of rationalization, as it involves dealing with unique or exceptional requirements.

upvoted 3 times

**Ashwin123** 5 months, 3 weeks ago

**Selected Answer: B**

A C & D are important considerations while rationalizing requirements

upvoted 1 times

**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: D**

It's D. When rationalizing privacy requirements to comply with various applicable laws and regulations, the main focus is typically on harmonizing shared obligations and privacy rights, implementing solutions that address shared needs, and applying the strictest standards to ensure compliance without violating other laws.

Option D suggests handling "outliers" (requirements that are unique to specific jurisdictions or laws) on a case-by-case basis, which is not a rational approach for aligning privacy requirements. Ideally, privacy programs aim for consistency and scalability by harmonizing common obligations and addressing any outliers through strategic planning, rather than ad hoc or case-by-case solutions.

upvoted 1 times

**Dhrumal** 7 months, 1 week ago

**Selected Answer: C**

harmonising to me is like taking a middle ground by only considering commonalities of various laws which is not a correct approach.

upvoted 1 times

**Rocketly** 11 months, 2 weeks ago

**Selected Answer: A**

A - it is not possible to harmonise different legislative frameworks. Instead, materially address all that apply, by applying the strictest standard, and treat outliers on a case-by-case basis

upvoted 2 times

**Habeeb007** 1 year ago

Correct Answer is A

upvoted 1 times

🗨️ 👤 **yzx666xming** 1 year ago

**Selected Answer: C**

C is another approach

upvoted 1 times

🗨️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: A**

The answer is A.

all other answers are included in the CIPM book under rationalisation. C as mentioned by others is incorrect. From cipm book - Another approach organizations employ, when possible, is to look to the strictest standard when seeking a solution, provided it does not violate any data privacy laws, exceed budgetary restrictions, or contradict organization goals and objectives.

upvoted 3 times

🗨️ 👤 **diogoffigueira** 1 year, 3 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗨️ 👤 **katzeti** 1 year, 4 months ago

C is correct

upvoted 3 times

🗨️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: B**

Rationalizing requirements primarily involves understanding and organizing the myriad obligations from different legislations and regulations, finding commonalities, and creating a unified approach that can meet the standards across the board. While implementing solutions is an outcome or a step post the rationalization process, it is not a direct part of the rationalization itself.

upvoted 3 times


What is the name for the privacy strategy model that describes delegated decision making?

- A. De-centralized.
- B. De-functionalized.
- C. Hybrid.
- D. Matrix.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

In a decentralized privacy strategy model, decision-making powers are delegated to various departments or units, rather than being centralized under a single entity or authority.

upvoted 1 times



Which of the following controls does the PCI DSS framework NOT require?

- A. Implement strong asset control protocols.
- B. Implement strong access control measures.
- C. Maintain an information security policy.
- D. Maintain a vulnerability management program.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

The Payment Card Industry Data Security Standard (PCI DSS) is specifically designed to ensure the safe handling of payment card data. The main focus is on aspects such as access controls, security policies, vulnerability management, etc. While asset control and management are important components of a robust information security program, PCI DSS doesn't specifically address "asset control protocols" in the same way it does the other listed measures.

upvoted 2 times

  **emily0922** 11 months ago

Correct answer, here is the evidence for reference: <https://www.youtube.com/watch?v=szVmMxWORBc>

upvoted 2 times


Which of the following privacy frameworks are legally binding?

- A. Binding Corporate Rules (BCRs).
- B. Generally Accepted Privacy Principles (GAPP).
- C. Asia-Pacific Economic Cooperation (APEC) Privacy Framework.
- D. Organization for Economic Co-Operation and Development (OECD) Guidelines.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

Binding Corporate Rules (BCRs) are designed for multinational corporations to transfer personal data internationally within the same corporate group to countries that do not ensure an adequate level of protection. BCRs, once approved by relevant data protection authorities, are legally binding.

upvoted 3 times

Which of the following is an example of Privacy by Design (PbD)?

- A. A company hires a professional to structure a privacy program that anticipates the increasing demands of new laws.
- B. The human resources group develops a training program for employees to become certified in privacy policy.
- C. A labor union insists that the details of employers' data protection methods be documented in a new contract.
- D. The information technology group uses privacy considerations to inform the development of new networking software.

**Suggested Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **Rocketly** 1 year ago

**Selected Answer: D**

Absolutely D - this is a standard example of PbD in action

upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 8 months ago

should be D

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: D**

Should be D

upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: D**

Privacy by Design (PbD) emphasizes integrating privacy considerations into the initial design and architecture of IT systems and business practices.

upvoted 1 times

🗳️ 👤 **DracoL** 2 years, 2 months ago

**Selected Answer: D**

only D is the answer. Privacy by Design dont document ... need to be build into the system, process

upvoted 2 times

🗳️ 👤 **DracoL** 2 years, 2 months ago

Should be D as per Luton. How can it be C. Doesnt make any sense

upvoted 1 times

🗳️ 👤 **Luton** 2 years, 2 months ago

Should be D

upvoted 2 times

🗳️ 👤 **FSampaio** 2 years, 3 months ago

Why not D? And, why C?

upvoted 2 times

In regards to the collection of personal data conducted by an organization, what must the data subject be allowed to do?

- A. Evaluate the qualifications of a third-party processor before any data is transferred to that processor.
- B. Obtain a guarantee of prompt notification in instances involving unauthorized access of the data.
- C. Set a time-limit as to how long the personal data may be stored by the organization.
- D. Challenge the authenticity of the personal data and have it corrected if needed.

**Suggested Answer: D**



Community vote distribution

D (100%)

  **katizeti** Highly Voted 2 years, 4 months ago

shouldn't be D?

upvoted 8 times

  **Boerenkool** Highly Voted 2 years, 4 months ago

Think it must be D. The controller defines the time to store. The data subject can request for erasure or object to the processing. But time limits can also be defined by law so this right cannot always be honoured

upvoted 6 times

  **Rocketly** Most Recent 1 year ago

Selected Answer: D

Data subject does not determine retention periods - the organisation decides and documents these. However individuals do have the right to challenge inaccuracies in their personal data and request rectification

upvoted 1 times

  **carlosbui** 1 year, 8 months ago

Should be D


upvoted 1 times

  **[Removed]** 1 year, 10 months ago

Selected Answer: D

Should be D

upvoted 1 times

  **Ssourav** 1 year, 10 months ago

Selected Answer: D

This right is commonly known as the "right to rectification." Data subjects should be able to ensure that their personal data is accurate and have the right to have inaccurate personal data rectified or completed if it is incomplete.

upvoted 2 times

  **creativesyde** 1 year, 11 months ago

D is the best answer



upvoted 2 times

  **DracoL** 2 years, 2 months ago

Selected Answer: D

D should be correct

upvoted 2 times

  **DracoL** 2 years, 2 months ago

again the answer give doesnt make any sense. Should be D.

upvoted 2 times

  **Luton** 2 years, 2 months ago

Should be D

upvoted 3 times

  **FSampaio** 2 years, 3 months ago

If it is Consent, could be C, but I think letter D should be right.  
upvoted 2 times



## SCENARIO -

Please use the following to answer the next question:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

Which is the best way to ensure that data on personal equipment is protected?

- A. User risk training.
- B. Biometric security.
- C. Encryption of the data.
- D. Frequent data backups.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Rocketly** 1 year ago

**Selected Answer: C**

Devices should always be encrypted to prevent unauthorised access  
upvoted 1 times

🗳️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: C**

Encryption of the data is the best way to ensure that data on personal equipment is protected, as it prevents unauthorized access to the data even if the equipment is lost or stolen. Encryption is the process of transforming data into an unreadable format that can only be decrypted with a valid key or password. Encryption can be applied to the entire device, a specific folder or file, or a removable storage media. Encryption is one of the most effective technical safeguards for data protection and is recommended by many privacy laws and standards.  
upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 8 months ago

Should be C  
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: C**

Should be C  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: C**

Encryption ensures that even if a device is lost or stolen, unauthorized individuals cannot easily access the data stored on the device without the proper decryption key or password.

upvoted 2 times

🗨️ 👤 **Alex951** 2 years, 1 month ago

It should be C

upvoted 3 times

🗨️ 👤 **DracoL** 2 years, 2 months ago

**Selected Answer: C**

Encrypt the data is the best and fastest possible way. Educating the user is also important but human error will happen.

upvoted 2 times

🗨️ 👤 **DracoL** 2 years, 2 months ago

Should be C. Best way to protect data on personal equipment is to Encrypt the data. User Risk training doesnt ensure that the data is protected, incident still can occur. Even best if the personal equipment is not only encrypted but remotely managed so that can do a remote wipe.

The answer again doesnt make any sense. Did Examtopic do a check?

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

From a business standpoint, what is the most productive way to view employee use of personal equipment for work-related tasks?

- A. The use of personal equipment is a cost-effective measure that leads to no greater security risks than are always present in a modern organization.
- B. Any computer or other equipment is company property whenever it is used for company business.
- C. While the company may not own the equipment, it is required to protect the business-related data on any equipment used by its employees.
- D. The use of personal equipment must be reduced as it leads to inevitable security risks.

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗳️ 👤 **Rocketly** 1 year ago

**Selected Answer: C**

C is pragmatic but still recognises the company's data ownership and accountability  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: C**

This perspective recognizes the reality of modern work environments, where Bring Your Own Device (BYOD) policies are becoming more common, while also emphasizing the company's responsibility to ensure data protection regardless of the device it resides on.  
upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

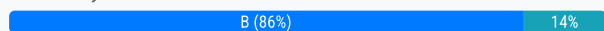
You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

In order to determine the best course of action, how should this incident most productively be viewed?

- A. As the accidental loss of personal property containing data that must be restored.
- B. As a potential compromise of personal information through unauthorized access.
- C. As an incident that requires the abrupt initiation of a notification campaign.
- D. As the premeditated theft of company data, until shown otherwise.

**Suggested Answer: B**

Community vote distribution



**humhain** 10 months, 3 weeks ago

**Selected Answer: B**

As a potential compromise of personal information through unauthorized access.  
upvoted 2 times

**katizeti** 11 months, 3 weeks ago

U think that B  
upvoted 1 times

**carlosbui** 1 year, 2 months ago

Should be B  
upvoted 1 times

**Ssourav** 1 year, 4 months ago

**Selected Answer: B**

Given the scenario, the primary concern is the potential compromise of client personal information due to the loss of the laptop. While other concerns may arise from the situation, protecting personal information and understanding the potential breach should be prioritized.  
upvoted 4 times

**emily0922** 1 year, 4 months ago

Should be B, should not identify as a data breach yet until confirmed, not sure if notification is required yet  
upvoted 2 times

**Adyyogi** 1 year, 5 months ago

**Selected Answer: C**

Because the laptop is not encrypted the best way is to assume a breach has happened and from here they should start the notification process  
upvoted 1 times



## SCENARIO -

Please use the following to answer the next question:

It's just what you were afraid of. Without consulting you, the information technology director at your organization launched a new initiative to encourage employees to use personal devices for conducting business. The initiative made purchasing a new, high-specification laptop computer an attractive option, with discounted laptops paid for as a payroll deduction spread over a year of paychecks. The organization is also paying the sales taxes. It's a great deal, and after a month, more than half the organization's employees have signed on and acquired new laptops. Walking through the facility, you see them happily customizing and comparing notes on their new computers, and at the end of the day, most take their laptops with them, potentially carrying personal data to their homes or other unknown locations. It's enough to give you data-protection nightmares, and you've pointed out to the information technology Director and many others in the organization the potential hazards of this new practice, including the inevitability of eventual data loss or theft.

Today you have in your office a representative of the organization's marketing department who shares with you, reluctantly, a story with potentially serious consequences. The night before, straight from work, with laptop in hand, he went to the Bull and Horn Pub to play billiards with his friends. A fine night of sport and socializing began, with the laptop "safely" tucked on a bench, beneath his jacket. Later that night, when it was time to depart, he retrieved the jacket, but the laptop was gone. It was not beneath the bench or on another bench nearby. The waitstaff had not seen it. His friends were not playing a joke on him. After a sleepless night, he confirmed it this morning, stopping by the pub to talk to the cleanup crew. They had not found it. The laptop was missing. Stolen, it seems. He looks at you, embarrassed and upset.

You ask him if the laptop contains any personal data from clients, and, sadly, he nods his head, yes. He believes it contains files on about 100 clients, including names, addresses and governmental identification numbers. He sighs and places his head in his hands in despair.

What should you do first to ascertain additional information about the loss of data?

- A. Interview the person reporting the incident following a standard protocol.
- B. Call the police to investigate even if you are unsure a crime occurred.
- C. Investigate the background of the person reporting the incident.
- D. Check company records of the latest backups to see what data may be recoverable.

**Suggested Answer: A**

Community vote distribution

A (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

The first step should be to gather more details about the incident from the person who reported it. This will help in understanding the nature and extent of the potential breach, the type of data that might be compromised, and the circumstances surrounding the loss.

upvoted 2 times

Which is NOT an influence on the privacy environment external to an organization?

- A. Management team priorities.
- B. Regulations.
- C. Consumer demand.
- D. Technological advances.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **Rocketly** 1 year ago

**Selected Answer: A**

Management team is an internal factor - not external  
upvoted 1 times

🗳️ 👤 **humhain** 1 year, 4 months ago

**Selected Answer: A**

Management team priorities.  
upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 8 months ago

Should be A  
upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: A**

Should be A  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: A**

Management team priorities are internal to an organization, whereas the other options are external factors that influence the privacy environment.  
upvoted 2 times

🗳️ 👤 **Adyyogi** 1 year, 11 months ago

Should ne A  
upvoted 3 times

🗳️ 👤 **Alex951** 2 years, 1 month ago

Should be A  
upvoted 3 times

🗳️ 👤 **Luton** 2 years, 2 months ago

Should be A. The only one that isn't external  
upvoted 4 times

How are individual program needs and specific organizational goals identified in privacy framework development?

- A. By employing metrics to align privacy protection with objectives.
- B. Through conversations with the privacy team.
- C. By employing an industry-standard needs analysis.
- D. Through creation of the business case.

**Suggested Answer:** D

Community vote distribution

D (88%)

13%

🗳️ 👤 **humhain** 10 months, 3 weeks ago

**Selected Answer: D**

The creation of the business case is the first step in privacy framework development, as it helps to identify the individual program needs and specific organizational goals. The business case is a document that outlines the rationale, objectives, benefits, costs, risks, and alternatives for implementing a privacy program. It also helps to communicate the value of privacy to stakeholders and gain their support. The other options are subsequent steps in privacy framework development, after the business case has been established.

upvoted 3 times

🗳️ 👤 **carlosbui** 1 year, 2 months ago

should be D

upvoted 1 times

🗳️ 👤 **DracoL** 1 year, 4 months ago

**Selected Answer: D**

under iAPP privacy framework development, first step is business case. So the answer is D.

upvoted 2 times

🗳️ 👤 **emily0922** 1 year, 4 months ago

Should be D, refer to the definition in the IAPP glossary for business case

upvoted 3 times

🗳️ 👤 **Adyyogi** 1 year, 5 months ago

**Selected Answer: A**

A, because a metric can reveal a need for improvement

upvoted 1 times

🗳️ 👤 **mgmferreira** 1 year, 7 months ago

**Selected Answer: D**

A criação de um caso de negócios para a estrutura de privacidade é uma maneira eficaz de identificar as necessidades individuais do programa e as metas organizacionais específicas.

upvoted 2 times



## SCENARIO -

Please use the following to answer the next question:

Natalia, the Chief Financial Officer (CFO) of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to question the company's privacy program at today's meeting.

Alice, a Vice President (VP), said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.

Spencer – a former Chief Executive Officer (CEO) and currently a senior advisor – said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.

One of the Business Development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.

Spencer replied that acting with reason means allowing security to be handled by the security functions within the company – not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.

Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month."

Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.

What is the most realistic step the organization can take to help diminish liability in the event of another incident?

- A. Requiring the vendor to perform periodic internal audits.
- B. Specifying mandatory data protection practices in vendor contracts.
- C. Keeping the majority of processing activities within the organization.
- D. Obtaining customer consent for any third-party processing of personal data.

**Suggested Answer: B**

Community vote distribution

B (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: B**

Specifying mandatory data protection practices in vendor contracts: By specifying certain practices in contracts, Nationwide Grill would establish a minimum threshold for security, making it clear what is expected from vendors in terms of data protection. This can also provide the company with a legal recourse in the event of a breach, thereby diminishing its liability.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Natalia, the Chief Financial Officer (CFO) of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to question the company's privacy program at today's meeting.

Alice, a Vice President (VP), said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.

Spencer – a former Chief Executive Officer (CEO) and currently a senior advisor – said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.

One of the Business Development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.

Spencer replied that acting with reason means allowing security to be handled by the security functions within the company – not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.

Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month."

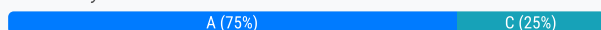
Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.

Based on the scenario, Nationwide Grill needs to create better employee awareness of the company's privacy program by doing what?

- A. Varying the modes of communication.
- B. Communicating to the staff more often.
- C. Improving inter-departmental cooperation.
- D. Requiring acknowledgment of company memos.

**Suggested Answer: A**

Community vote distribution



**ShadyB** 4 months, 2 weeks ago

**Selected Answer: A**

A. Varying the modes of communication.

The scenario highlights that employees are overwhelmed by the sheer volume and duplication of information from HR and the ethics department. This indicates a problem with the method of communication, not necessarily the frequency or content.

Varying the modes of communication could include: 1) Short, engaging videos. 2) Interactive online training modules. 3) Gamified learning experiences.

Concise, visually appealing infographics. 4) Targeted micro learning.

Here's why the other options are less effective in this specific scenario:

C. Inter-departmental: While inter-departmental cooperation is generally a good idea, it doesn't directly address the issue of information overload and ineffective communication.

D. Acknowledgment: This might ensure that employees see the memos, but it doesn't guarantee that they understand or retain the information. It also adds to the information overload.

upvoted 1 times

**Vinz\_** 6 months, 4 weeks ago

**Selected Answer: C**

Varying the modes of communications would unlikely improve the Privacy programme since the scenario reported the presence of multiple communication channels. HR and Ethics department should coordinate with the security function as well as other departments to identify the necessary training material tailored to different roles, hence increasing interest and ultimately privacy awareness.

upvoted 1 times

  **Dhrumal** 7 months ago

**Selected Answer: C**

I thought of C as HR and Ethics department both were bombarding employees with information which led to overload of information for employees and they started ignoring the messages.

upvoted 1 times

  **kuca11** 7 months, 3 weeks ago

D, Requiring acknowledgment of company memos as the circumstances mention states "Both the volume and the duplication of information means that it is often ignored altogether."

upvoted 1 times

  **katizeti** 1 year, 5 months ago

In my opinion A is correct

upvoted 2 times

  **carlosbui** 1 year, 8 months ago

Should be A

upvoted 2 times

  **Ssourav** 1 year, 10 months ago

**Selected Answer: A**


Varying the modes of communication: If employees are overwhelmed with emails, memos, and posters, using a variety of methods such as interactive training sessions, videos, or team discussions could improve engagement and retention of information.

upvoted 3 times

  **emily0922** 1 year, 11 months ago

I think should be C "He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether."

upvoted 1 times

  **Adyyogi** 1 year, 11 months ago

**Selected Answer: A**

A, because varying the way communication is delivered means that you adapt the content and delivery to the audience, which is the appropriate way

upvoted 2 times

  **Larryqwe** 2 years, 3 months ago

Or answer a?

upvoted 1 times

  **Boerenkool** 2 years, 4 months ago

Why not C?

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Natalia, the Chief Financial Officer (CFO) of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to question the company's privacy program at today's meeting.

Alice, a Vice President (VP), said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.

Spencer – a former Chief Executive Officer (CEO) and currently a senior advisor – said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.

One of the Business Development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.

Spencer replied that acting with reason means allowing security to be handled by the security functions within the company – not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.

Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month."

Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.

How could the objection to Spencer's training suggestion be addressed?

- A. By requiring training only on an as-needed basis.
- B. By offering alternative delivery methods for trainings.
- C. By introducing a system of periodic refresher trainings.
- D. By customizing training based on length of employee tenure.

**Suggested Answer: B**

Community vote distribution

B (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: B**

Offering alternative delivery methods, such as online modules or webinars, could allow for flexibility in when and where training is completed. This would be especially useful for an organization like Nationwide Grill, which has multiple locations and likely varying schedules among employees.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Natalia, the Chief Financial Officer (CFO) of the Nationwide Grill restaurant chain, had never seen her fellow executives so anxious. Last week, a data processing firm used by the company reported that its system may have been hacked, and customer data such as names, addresses, and birthdays may have been compromised. Although the attempt was proven unsuccessful, the scare has prompted several Nationwide Grill executives to question the company's privacy program at today's meeting.

Alice, a Vice President (VP), said that the incident could have opened the door to lawsuits, potentially damaging Nationwide Grill's market position. The Chief Information Officer (CIO), Brendan, tried to assure her that even if there had been an actual breach, the chances of a successful suit against the company were slim. But Alice remained unconvinced.

Spencer – a former Chief Executive Officer (CEO) and currently a senior advisor – said that he had always warned against the use of contractors for data processing. At the very least, he argued, they should be held contractually liable for telling customers about any security incidents. In his view, Nationwide Grill should not be forced to soil the company name for a problem it did not cause.

One of the Business Development (BD) executives, Haley, then spoke, imploring everyone to see reason. "Breaches can happen, despite organizations' best efforts," she remarked. "Reasonable preparedness is key." She reminded everyone of the incident seven years ago when the large grocery chain Tinkerton's had its financial information compromised after a large order of Nationwide Grill frozen dinners. As a long-time BD executive with a solid understanding of Tinkerton's corporate culture, built up through many years of cultivating relationships, Haley was able to successfully manage the company's incident response.

Spencer replied that acting with reason means allowing security to be handled by the security functions within the company – not BD staff. In a similar way, he said, Human Resources (HR) needs to do a better job training employees to prevent incidents. He pointed out that Nationwide Grill employees are overwhelmed with posters, emails, and memos from both HR and the ethics department related to the company's privacy program. Both the volume and the duplication of information means that it is often ignored altogether.

Spencer said, "The company needs to dedicate itself to its privacy program and set regular in-person trainings for all staff once a month."

Alice responded that the suggestion, while well-meaning, is not practical. With many locations, local HR departments need to have flexibility with their training schedules. Silently, Natalia agreed.

The senior advisor, Spencer, has a misconception regarding?

- A. The amount of responsibility that a data controller retains.
- B. The appropriate role of an organization's security department.
- C. The degree to which training can lessen the number of security incidents.
- D. The role of Human Resources employees in an organization's privacy program.

**Suggested Answer: A**

Community vote distribution

A (100%)

 **Ssourav** Highly Voted 1 year, 4 months ago

**Selected Answer: A**

This answer reflects Spencer's sentiment that Nationwide Grill shouldn't be accountable for a third party's actions. Even if a third party (data processor) is involved, the primary organization (data controller) still retains a significant amount of responsibility for data protection and ensuring that third-party processors are compliant with data protection standards.

upvoted 5 times

 **Dhruval** Most Recent 7 months ago

**Selected Answer: A**

Ultimate responsibility of privacy lies with data controller.

upvoted 1 times

 **katizeti** 11 months, 3 weeks ago


I think that it may be B. Spencer, has a misconception regarding the appropriate role of an organization's security department. Spencer believes that security should be handled by the security functions within the company, not by the business development staff. However, it's important to ensure that employees are aware of the risks and take necessary precautions to secure their devices.

upvoted 1 times

 **carlosbui** 1 year, 2 months ago

should be A

upvoted 1 times

  **Adyyogi** 1 year, 5 months ago

**Selected Answer: A**

Should be A



upvoted 2 times

  **Alex951** 1 year, 7 months ago

**Selected Answer: A**

Should be A

upvoted 3 times

  **Luton** 1 year, 8 months ago

**Selected Answer: A**

Should be A

upvoted 2 times

Formosa International operates in 20 different countries including the United States and France.  
What organizational approach would make complying with a number of different regulations easier?

- A. Data mapping.
- B. Fair Information Practices.
- C. Rationalizing requirements.
- D. Decentralized privacy management.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **humhain** 10 months, 3 weeks ago

**Selected Answer: C**

Rationalizing requirements is an organizational approach that involves identifying and harmonizing the common elements of different privacy regulations and standards. This can make compliance easier and more efficient, as well as reduce the risk of conflicts or gaps in privacy protection. Rationalizing requirements can also help to create a consistent privacy policy and culture across different jurisdictions and business units.

upvoted 3 times

🗳️ 👤 **carlosbui** 1 year, 2 months ago

should be C

upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: C**

Rationalizing requirements involves harmonizing shared obligations and privacy rights across varying legislation and/or regulators. It means implementing solutions that address shared obligations and standards, applying the strictest standards where they don't conflict with other laws, and addressing outliers on a case-by-case basis. This approach can help an organization navigate the complexities of multiple privacy regimes in an efficient manner.

upvoted 3 times

🗳️ 👤 **DracoL** 1 year, 8 months ago

**Selected Answer: C**

should be C. When spanning across countries, should rationalise the policies not fair information practise.

upvoted 1 times

🗳️ 👤 **Luton** 1 year, 8 months ago

Should be C

upvoted 2 times

🗳️ 👤 **Boerenkool** 1 year, 10 months ago

Why not c?

upvoted 1 times


When implementing Privacy by Design (PbD), what would NOT be a key consideration?

- A. Collection limitation.
- B. Data minimization.
- C. Limitations on liability.
- D. Purpose specification.

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **Ssourav** 10 months, 3 weeks ago

**Selected Answer:** C

Privacy by Design primarily focuses on proactively integrating privacy considerations into the design and operation of systems, projects, and processes. Elements like collection limitation, data minimization, and purpose specification are foundational to the PbD framework. Limitations on liability, while important in a legal or contractual context, are not a core element of designing a system with privacy considerations at the forefront.

upvoted 1 times

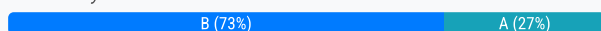


For an organization that has just experienced a data breach, what might be the least relevant metric for a company's privacy and governance team?

- A. The number of security patches applied to company devices.
- B. The number of privacy rights requests that have been exercised.
- C. The number of Privacy Impact Assessments that have been completed.
- D. The number of employees who have completed data awareness training.

**Suggested Answer: B**

Community vote distribution



🗳️ **daniel.ross.1919** 9 months, 3 weeks ago

B. This may well be immaterial and unrelated.  
upvoted 1 times

🗳️ **MaritzTee** 1 year, 1 month ago

**Selected Answer: B**

B. The number of privacy rights requests that have been exercised.

In the context of an organization that has just experienced a data breach, the least relevant metric for a company's privacy and governance team would likely be the number of privacy rights requests that have been exercised. This metric pertains more to the ongoing management of data subject rights under privacy laws (such as GDPR or CCPA) rather than the immediate response and mitigation efforts following a data breach. The other metrics directly relate to the organization's security posture and preparedness, which are more critical in addressing the aftermath of a breach.

upvoted 1 times

🗳️ **DPRamone** 1 year, 4 months ago

**Selected Answer: B**

A, C, and D provide metrics providing clues as to where gaps contributing to the breach may be identified. B doesn't.  
upvoted 2 times

🗳️ **humhain** 1 year, 4 months ago

**Selected Answer: A**

The number of security patches applied to company devices might be the least relevant metric for a company's privacy and governance team after a data breach. While security patches are important for preventing future breaches, they do not directly measure the impact or response of the current breach. The other metrics are more relevant for assessing how the company handled the breach, such as how it complied with the privacy rights of affected individuals, how it evaluated the privacy risks of its systems, and how it trained its employees on data awareness.

upvoted 1 times

🗳️ **carlosbui** 1 year, 8 months ago

should be A  
upvoted 1 times

🗳️ **[Removed]** 1 year, 10 months ago

**Selected Answer: B**

Should be B  
upvoted 1 times

🗳️ **Ssourav** 1 year, 10 months ago

**Selected Answer: B**



While privacy rights requests (like data access or deletion requests) are important indicators of how an organization is responding to data subject rights, they do not directly address the factors leading to or mitigating a data breach. The other metrics listed pertain more directly to preventative measures or understanding vulnerabilities.

upvoted 4 times

🗳️ **Adyyogi** 1 year, 11 months ago

Governance, risk, and compliance tools (GRC) is an umbrella term whose scope touches the privacy office, as well as other departments, including HR, IT, compliance, and the C-suite. But A is the answer

upvoted 1 times

  **DracoL** 2 years, 2 months ago

**Selected Answer: A**

A is correct. Vulnerabilities tracking should be a cyber security responsibilities.

upvoted 2 times

In which situation would a Privacy Impact Assessment (PIA) be the least likely to be required?

- A. If a company created a credit-scoring platform five years ago.
- B. If a health-care professional or lawyer processed personal data from a patient's file.
- C. If a social media company created a new product compiling personal data to generate user profiles.
- D. If an after-school club processed children's data to determine which children might have food allergies.

**Suggested Answer: A**

Community vote distribution

A (50%)

B (50%)

 **Ssourav**  1 year, 4 months ago

**Selected Answer: B**

In many jurisdictions, the processing of personal data by health-care professionals and lawyers as part of their regular professional duties (for instance, treatment of patients or legal representation) might not necessarily trigger the requirement for a PIA. This is because the processing is generally understood, expected, and subject to other professional and legal obligations, like doctor-patient or attorney-client confidentiality.  
upvoted 5 times

 **Vinz\_**  7 months ago

**Selected Answer: A**

Correct answer is A, because that is an old project and it is less likely compared to the other answers to require a PIA. All the other answers include sensitive personal data and / or new technologies  
upvoted 2 times

 **Dhruval** 7 months ago

**Selected Answer: B**

healthcare professional or lawyer if not processing sensitive personal data on large scale then they are not required to do DPIA.  
upvoted 1 times

 **humhain** 10 months, 3 weeks ago

**Selected Answer: A**


A Privacy Impact Assessment (PIA) is a process that helps to identify and mitigate the privacy risks of a project or activity that involves personal data. A PIA is usually required when there is a new or significant change in the way personal data is collected, used, or disclosed. Therefore, a PIA would be the least likely to be required if a company created a credit-scoring platform five years ago, as this would not be a new or significant change. The other situations involve new or changed processing of personal data that could have privacy impacts, such as sensitive data (health or children's data), profiling data (user profiles), or large-scale data (patient's file).  
upvoted 3 times

 **carlosbui** 1 year, 2 months ago

should be B  
upvoted 1 times


 **Adyyogi** 1 year, 5 months ago

Privacy assessments measure an organization's compliance with laws, regulations, adopted standards, and internal policies and procedures. Their scope may include education and awareness; monitoring and responding to the regulatory environment; data, systems, and process assessments; risk assessments; incident response; contracts; remediation; and program assurance, including audits.  
upvoted 1 times

 **Boats** 1 year, 6 months ago

**Selected Answer: A**

PIAs are triggered do to some type of new activity. New data being added, new database, new program. A should be the correct answer because a PIA should have been done five years ago.  
upvoted 1 times

 **tonik** 1 year, 7 months ago

B maybe?

upvoted 2 times

Under the General Data Protection Regulation (GDPR), what must be included in a written agreement between the controller and processor in relation to processing conducted on the controller's behalf?

- A. An obligation on the processor to report any personal data breach to the controller within 72 hours.
- B. An obligation on both parties to report any serious personal data breach to the supervisory authority.
- C. An obligation on both parties to agree to a termination of the agreement if the other party is responsible for a personal data breach.
- D. An obligation on the processor to assist the controller in complying with the controller's obligations to notify the supervisory authority about personal data breaches.

**Suggested Answer: D**

Community vote distribution

D (80%)

A (20%)

🗳️ 👤 **thecheaterz** 7 months, 4 weeks ago

**Selected Answer: D**

Not A, this is to be agreed between the contracting parties. 72 hours reporting relates to notifying the SA.  
upvoted 2 times

🗳️ 👤 **humhain** 10 months, 3 weeks ago

**Selected Answer: A**

An obligation on the processor to report any personal data breach to the controller within 72 hours.  
upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 2 months ago

should be D  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: D**

Art 28 3 (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; that includes data breach notification  
upvoted 2 times

🗳️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: A**

Article 28 of the GDPR specifies the details that should be included in the contract between the controller and the processor. One of these is the obligation on the processor to notify the controller without undue delay upon becoming aware of a personal data breach. The exact timeframe (like the 72 hours) is not specified in this context in Article 28, but the principle of notifying the controller without undue delay is there.  
upvoted 1 times

🗳️ 👤 **DracoL** 1 year, 4 months ago

**Selected Answer: D**

Controller need to notified regulator and data subject wihin 72 hours. So the data processor need to inform controller a lot faster and assist the controller obligations.  
upvoted 4 times

🗳️ 👤 **emily0922** 1 year, 5 months ago

Should be D  
upvoted 2 times

🗳️ 👤 **prathibs** 1 year, 5 months ago

It is D  
upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers. Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What does this example best illustrate about training requirements for privacy protection?

- A. Training needs must be weighed against financial costs.
- B. Training on local laws must be implemented for all personnel.
- C. Training must be repeated frequently to respond to new legislation.
- D. Training must include assessments to verify that the material is mastered.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

 **Cock** 8 months, 1 week ago

**Selected Answer: B**

This example best illustrates the importance of B. Training on local laws must be implemented for all personnel. It highlights the significance of ensuring that employees are aware of and trained on local privacy laws and regulations to avoid legal and compliance issues.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers. Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

Knowing that the regulator is now investigating, what would be the best step to take?

- A. Consult an attorney experienced in privacy law and litigation.
- B. Use your background and knowledge to set a course of action.
- C. If you know the organization is guilty, advise it to accept the punishment.
- D. Negotiate the terms of a settlement before formal legal action takes place.

**Suggested Answer: A**

Currently there are no comments in this discussion, be the first to comment!

## SCENARIO -

Please use the following to answer the next question:

Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain "rogue" offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.

In the wake of this incident, Kelly had been sent to Providence to change the "hands off" culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers. Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.

Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.

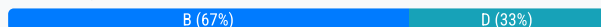
You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.

What should you advise this company regarding the status of security cameras at their offices in the United States?

- A. Add security cameras at facilities that are now without them.
- B. Set policies about the purpose and use of the security cameras.
- C. Reduce the number of security cameras located inside the building.
- D. Restrict access to surveillance video taken by the security cameras and destroy the recordings after a designated period of time.

**Suggested Answer: B**

*Community vote distribution*



🗳️ **katizeti** 11 months, 3 weeks ago

B should be correct  
upvoted 1 times

🗳️ **Cock** 1 year, 2 months ago

**Selected Answer: B**

In US is B. Set policies about the purpose and use of the security cameras. It's crucial to establish clear guidelines and policies regarding the use of security cameras to ensure they are used for legitimate security purposes and comply with privacy regulations.  
upvoted 2 times

🗳️ **tonik** 1 year, 7 months ago

**Selected Answer: D**

...in EU is D  
upvoted 1 times

🗳️ **DPRamone** 10 months ago

The question explicitly states the offices in the US.  
upvoted 1 times



You would like your organization to be independently audited to demonstrate compliance with international privacy standards and to identify gaps for remediation.

Which type of audit would help you achieve this objective?

- A. First-party audit.
- B. Second-party audit.
- C. Third-party audit.
- D. Fourth-party audit.

**Suggested Answer:** *C*

Currently there are no comments in this discussion, be the first to comment!

An organization's business continuity plan or disaster recovery plan does NOT typically include what?

- A. Recovery time objectives.
- B. Emergency response guidelines.
- C. Statement of organizational responsibilities.
- D. Retention schedule for storage and destruction of information.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

## SCENARIO -

Please use the following to answer the next question:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

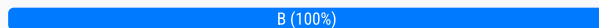
Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

Since it is too late to restructure the contract with the vendor or prevent the app from being deployed, what is the best step for you to take next?

- A. Implement a more comprehensive suite of information security controls than the one used by the vendor.
- B. Ask the vendor for verifiable information about their privacy protections so weaknesses can be identified.
- C. Develop security protocols for the vendor and mandate that they be deployed.
- D. Insist on an audit of the vendor's privacy procedures and safeguards.

**Suggested Answer: B**

*Community vote distribution*



 **DPRamone** 10 months, 1 week ago

**Selected Answer: B**

"Since it is too late to restructure the contract with the vendor ...": the right to audit is generally part of the contract. If it's not in there, B makes sense.  
upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

Which is the best first step in understanding the data security practices of a potential vendor?

- A. Requiring the vendor to complete a questionnaire assessing International Organization for Standardization (ISO) 27001 compliance.
- B. Conducting a physical audit of the vendor's facilities.
- C. Conducting a penetration test of the vendor's data security structure.
- D. Examining investigation records of any breaches the vendor has experienced.

**Suggested Answer: A**



Community vote distribution

A (100%)

  **carlosbui** 8 months ago

should be A

upvoted 1 times

  **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

A questionnaire assessing the vendor's compliance with ISO 27001 would provide a comprehensive overview of the vendor's information security practices. This initial step is less intrusive and resource-intensive than some of the other options and serves as a good starting point for understanding the vendor's security posture.

upvoted 2 times

  **Adyyogi** 11 months ago

**Selected Answer: A**

" data security practices" probably refer to cyber security measures, not to physical security measure...so I choose A

upvoted 2 times

  **Alex951** 1 year ago

**Selected Answer: A**

typo, should be A

upvoted 3 times

  **Alex951** 1 year, 1 month ago

I suggest B

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

What safeguard can most efficiently ensure that privacy protection is a dimension of relationships with vendors?

- A. Include appropriate language about privacy protection in vendor contracts.
- B. Perform a privacy audit on any vendor under consideration.
- C. Require that a person trained in privacy protection be part of all vendor selection teams.
- D. Do business only with vendors who are members of privacy trade associations.

## Suggested Answer: A

Community vote distribution

A (100%)

 **humhain** 10 months, 3 weeks ago

**Selected Answer: A**

This answer is the best way to ensure that privacy protection is a dimension of relationships with vendors, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for data processing activities. Including appropriate language about privacy protection in vendor contracts can help to define the scope, purpose, duration and type of data processing, as well as the rights and obligations of both parties. The contracts can also specify the technical and organizational measures that the vendor must implement to protect the data from unauthorized or unlawful access, use, disclosure, alteration or destruction, and to notify the organization of any security incidents or breaches. The contracts can also allow the organization to monitor, audit or inspect the vendor's performance and compliance with the contract terms and applicable laws and regulations.


upvoted 1 times

 **Ssourav** 1 year, 4 months ago

**Selected Answer: A**

By embedding privacy protection clauses directly into vendor contracts, organizations can establish clear expectations and legally binding obligations for vendors to adhere to privacy standards and practices. This provides a framework for accountability and sets the baseline requirements for privacy protection. While the other options have their merits, embedding requirements directly into contracts is a scalable and efficient way to ensure privacy protection across multiple vendor relationships.

upvoted 4 times

 **Gh789** 1 year, 4 months ago

Should be A

upvoted 2 times

 **Alex951** 1 year, 7 months ago

Should be A I guess?

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

You want to point out that normal protocols have NOT been followed in this matter.

Which process in particular has been neglected?

- A. Forensic inquiry.
- B. Data mapping.
- C. Privacy breach prevention.
- D. Vendor due diligence or vetting.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

## SCENARIO -

Please use the following to answer the next question:

Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.

This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. "It's going to be great," the developer, Deidre Hoffman, tells you, "if, that is, we actually get it working!" She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. "It's just three young people," she says, "but they do great work." She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. "They do good work, so I chose them."

Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, "I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!"

You see evidence that company employees routinely circumvent the privacy officer in developing new initiatives.


How can you best draw attention to the scope of this problem?

- A. Insist upon one-on-one consultation with each person who works around the privacy officer.
- B. Develop a metric showing the number of initiatives launched without consultation and include it in reports, presentations, and consultation.
- C. Hold discussions with the department head of anyone who fails to consult with the privacy officer.
- D. Take your concerns straight to the Chief Executive Officer.

**Suggested Answer: B**

Community vote distribution

B (100%)

 **katizeti** 11 months, 3 weeks ago


I think that B is correct

upvoted 1 times

 **carlosbui** 1 year, 2 months ago

should be B

upvoted 1 times

 **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

Metrics provide quantifiable data that can be used to demonstrate the extent of a problem. By illustrating how often initiatives are launched without the proper consultation, this is way of providing clear evidence of the gap in the process. It's a data-driven approach that can be effectively communicated to stakeholders and can help to instill the importance of privacy consultation in future initiatives.

upvoted 3 times

 **emily0922** 1 year, 5 months ago

Should be B

upvoted 2 times



What is one obligation that the General Data Protection Regulation (GDPR) imposes on data processors?

- A. To honor all data access requests from data subjects.
- B. To inform data subjects about the identity and contact details of the controller.
- C. To implement appropriate technical and organizational measures that ensure an appropriate level of security.
- D. To carry out data protection impact assessments in cases where processing is likely to result in high risk to the rights and freedoms of individuals.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Boerenkool** Highly Voted 1 year, 10 months ago

Should be C. In Gdpr the controller must execute the dpia, not the processor  
upvoted 5 times

🗳️ 👤 **giomike** Most Recent 11 months, 1 week ago

C:\ One obligation that the General Data Protection Regulation (GDPR) imposes on data processors is the requirement to implement appropriate technical and organizational measures to ensure the security of personal data. This includes measures such as encryption, pseudonymization, and regular testing and evaluation of the effectiveness of security measures.  
upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 2 months ago

should be C  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 4 months ago

Selected Answer: C

Art 32 (1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:  
upvoted 2 times

🗳️ 👤 **AlwinL** 1 year, 8 months ago

Ans should be C. Art. 32 GDPR - Security of processing  
upvoted 3 times

🗳️ 👤 **bilgecell** 1 year, 8 months ago

Hi, Article 35 of the GDPR, Processors must carry out DPIA under some conditions such as processing sensitive data, the use of new tech, processing health data , protecting of public health, large-scale processing of personal data.  
upvoted 1 times

🗳️ 👤 **sham222** 1 year, 8 months ago

Selected Answer: C

Under GDPR, data processors have an obligation to implement appropriate technical and organizational measures that ensure an appropriate level of security for personal data, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. This includes measures such as pseudonymization and encryption of personal data, ensuring the confidentiality, integrity, availability, and resilience of processing systems and services, and regularly testing, assessing, and evaluating the effectiveness of security measures.  
upvoted 4 times

An executive for a multinational online retail company in the United States is looking for guidance in developing her company's privacy program beyond what is specifically required by law.

What would be the most effective resource for the executive to consult?

- A. Internal auditors.
- B. Industry frameworks.
- C. Oversight organizations.
- D. Breach notifications from competitors.

**Suggested Answer:** *B*

Currently there are no comments in this discussion, be the first to comment!

What is one reason the European Union has enacted more comprehensive privacy laws than the United States?

- A. To ensure adequate enforcement of existing laws.
- B. To ensure there is adequate funding for enforcement.
- C. To allow separate industries to set privacy standards.
- D. To allow the free movement of data between member countries.

**Suggested Answer:** *D*

Currently there are no comments in this discussion, be the first to comment!

All of the following changes will likely trigger a data inventory update EXCEPT?

- A. Outsourcing the Customer Relationship Management (CRM) function.
- B. Acquisition of a new subsidiary.
- C. Onboarding of a new vendor.
- D. Passage of a new privacy regulation.

**Suggested Answer: D**

*Community vote distribution*

D (100%)

🗳️ 👤 **carlosbui** 8 months ago

should be D

upvoted 1 times

🗳️ 👤 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: D**

While a new privacy regulation might necessitate a review of data handling practices, privacy policies, and compliance measures, it doesn't inherently change the data inventory itself. The other options (A, B, and C) involve changes to the actual data landscape of the organization, necessitating updates to the data inventory.

upvoted 3 times

🗳️ 👤 **Adyyogi** 11 months ago

**Selected Answer: D**

D is the only logical one correct

upvoted 2 times

🗳️ 👤 **mgmferreira** 1 year, 1 month ago

**Selected Answer: D**

Letra D

upvoted 2 times

🗳️ 👤 **bilgecell** 1 year, 2 months ago

A is correct. Data inventory is affected by regulations. According to the regulations, the retention periods of the data or the measures to be taken may change or new articles may be added to the legal basis of data processing.

upvoted 1 times

🗳️ 👤 **Adyyogi** 11 months ago

Data inventory already exists, and is correctly done, so new developed regulation does not modify the content of the inventory ...

upvoted 1 times

🗳️ 👤 **Adyyogi** 11 months ago

but can add new requirements...

upvoted 1 times

🗳️ 👤 **DracoL** 1 year, 2 months ago

**Selected Answer: D**

data inventory is a better answer cause introduction of new regulation doesnt impact the existing data sets except implement different security, access control on data sets

upvoted 3 times

🗳️ 👤 **Luton** 1 year, 2 months ago

Should be D

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert."

Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks, espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts."

The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A "cleaning crew" of one teenager is emptying the trash bins. A few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!"

What would be the best kind of audit to recommend for Gadgo?

- A. A supplier audit.
- B. An internal audit.
- C. A third-party audit.
- D. A self-certification.

**Suggested Answer: C**

Community vote distribution

C (71%)

B (29%)

🗳️ 👤 **9385ae2** 5 months, 3 weeks ago

**Selected Answer: C**

C. need an independent third party to complete this.

upvoted 1 times

🗳️ 👤 **Vinz\_** 6 months, 2 weeks ago

**Selected Answer: C**

First party audits usually support self certifications and there is no clue in the described scenario that an internal audit team exists. Third party audits are independent and provide a level of expert recommendations.

upvoted 1 times

🗳️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: B**

Also let me add this. The IAPP CIPM framework emphasizes the importance of conducting internal assessments to evaluate privacy and security risks, especially when a company has gaps in its data protection practices. Given that the scenario describes Gadgo as a company with inconsistent controls, lax data protection measures, and informal privacy practices, an internal audit provides the best foundation for addressing those issues.

upvoted 1 times

🗳️ 👤 **9385ae2** 6 months ago

Disagree. Should be C. Who has the expertise, internally, to the audit. Surely they don't have the right person/people on staff to complete an internal audit.

upvoted 1 times

🗳️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: B**

It's B. Here's why: Given the state of the company's privacy and security measures, an internal audit is the best way to assess current practices, identify gaps, and help develop stronger controls and procedures. This audit will also assist in educating the leadership (including both Paul and

Carlton) on the necessary steps to protect the company's data. Given that the company appears to be missing fundamental privacy and security structures, an internal audit would be an appropriate first step before seeking external guidance or compliance certifications.

upvoted 1 times

🗨️ 👤 **Adyyogi** 11 months ago

**Selected Answer: C**

third party audit will be most likely accepted by anyone as objective

upvoted 3 times

🗨️ 👤 **bilgecell** 1 year, 2 months ago

In this scenario, an external audit may be a good option to persuade the management body and get objective feedback.

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. "Carlton won't listen to me," Paul says, "but he may pay attention to an expert."

Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks. espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. "This is a technology company," Carlton says. "We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts."

The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A "cleaning crew" of one teenager is emptying the trash bins. A few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: "Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!"

What phase in the Privacy Maturity Model (PMM) does Gadgo's privacy program best exhibit?

- A. Ad hoc.
- B. Defined.
- C. Repeatable.
- D. Managed.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗲️ 👤 **Adyyogi** 11 months ago

**Selected Answer: A**

...close to nothing implemented

upvoted 1 times

🗲️ 👤 **bilgecell** 1 year, 2 months ago

A is correct.

The AICPA/CICA Privacy Maturity Model is based on GAPP and the Capability Maturity Model (CMM). The PMM uses five maturity levels as follows:

Ad hoc: Procedures or processes are generally informal, incomplete, and inconsistently applied

Repeatable: Procedures or processes exist; however, they are not fully documented and do not cover all relevant aspects

Defined: Procedures and processes are fully documented and implemented and cover all relevant aspects

Managed: Reviews are conducted to assess the effectiveness of the controls in place

Optimized: Regular review and feedback are used to ensure continuous improvement towards optimization of the given process

upvoted 4 times

Incipia Corporation just trained the last of its 300 employees on their new privacy policies and procedures.

If Incipia wanted to analyze the effectiveness of the training over the next 6 months, which form of trend analysis should they use?

- A. Cyclical.
- B. Irregular.
- C. Statistical.
- D. Standard variance.

**Suggested Answer: C**

Community vote distribution

C (71%)

A (29%)

44d06fe 3 months, 3 weeks ago

**Selected Answer: A**

From IAPP book : A second form of analysis is called "cyclical component," which shows data over a period focused on regular fluctuations.

Measuring the number of incident responses in the month after an organization rolls out new privacy training, this analysis is focused on explaining any changes in the number of reported incidents as the distance from training increases.

upvoted 1 times

HaraTadahisa 1 year ago

**Selected Answer: C**

It must be C.

upvoted 1 times

0d0ded9 1 year ago

A. Measures the number of privacy breaches over a period after an organization rolls out new privacy training.

upvoted 1 times

thecheaterz 1 year, 1 month ago

**Selected Answer: A**

A second form of analysis is called "cyclical component," which shows data over a period focused on regular fluctuations. Measuring the number of incident responses in the month after an organization rolls out new privacy training, this analysis is focused on explaining any changes in the number of reported incidents as the distance from training increases.

upvoted 1 times

humhain 1 year, 4 months ago

**Selected Answer: C**

This answer is the best form of trend analysis that Incipia Corporation should use to analyze the effectiveness of the training over the next six months, as it can provide a quantitative and objective way to measure and compare the results and outcomes of the training against predefined criteria or indicators. Statistical trend analysis is a method that involves collecting, analyzing and presenting data using statistical tools and techniques, such as charts, graphs, tables or formulas. Statistical trend analysis can help to identify patterns, changes or correlations in the data over time, as well as to evaluate the performance and impact of the training on the organization's privacy program and objectives.

upvoted 2 times

Gh789 1 year, 10 months ago

Cyclical Analysis

upvoted 1 times



Ssourav 1 year, 10 months ago

**Selected Answer: C**

This approach would involve collecting data related to the privacy policies and procedures and analyzing them using statistical methods to determine if the training has had a measurable effect. For instance, if the number of privacy-related incidents decreased post-training, a statistical analysis could help determine if the decrease is significant or just a random variation.



upvoted 2 times

  **Gh789** 1 year, 10 months ago

Cyclical analysis, option A

upvoted 1 times

  **emily0922** 1 year, 11 months ago

Should be A

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.

One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.

Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.

To determine the steps to follow, what would be the most appropriate internal guide for Ben to review?

- A. Incident Response Plan.
- B. Code of Business Conduct.
- C. IT Systems and Operations Handbook.
- D. Business Continuity and Disaster Recovery Plan.

**Suggested Answer: A**

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: A**

The most appropriate internal guide for Ben to review in order to determine the steps to follow after noticing unusual activity on company files would be: A. Incident Response Plan.

upvoted 2 times

🗳️ 👤 **DracoL** 11 months ago

**Selected Answer: A**

I agree with A. This case is obviously under the Response Phase (Protect) and under the CIPM material, one of the section of response phase is Incident Response Plan.

upvoted 2 times

🗳️ 👤 **Adyyogi** 11 months ago

**Selected Answer: A**

A\_ because in the incident Mng Plan should be included steps to follow in these situations. Now..."Codes of conduct are not obligatory but rather potential tools that can be used to promote compliance. Article 40 GDPR elaborates upon a pre-existing provision under the Directive 95/46/EC (Data Protection Directive – DPD), specifically Article 27(1)..." CoC relates more to B2B relationship than "employee to employer"..

upvoted 3 times

🗳️ 👤 **creativesyde** 11 months, 2 weeks ago

This should be A

upvoted 2 times

🗳️ 👤 **Alex951** 1 year, 1 month ago

This should definitely be incident response plan

upvoted 2 times

🗳️ 👤 **bilgecell** 1 year, 2 months ago

I selected incident response plan but correct answer is code of conduct. I haven't seen code of conduct sample but there is an explanation at GDPR. You can glance at [https://gdprhub.eu/Article\\_40\\_GDPR](https://gdprhub.eu/Article_40_GDPR). It seems a standard includes all data privacy life cycle.

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.

One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.

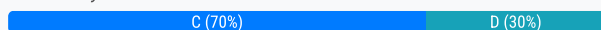
Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.

If this were a data breach, how is it likely to be categorized?

- A. Availability Breach.
- B. Authenticity Breach.
- C. Confidentiality Breach.
- D. Integrity Breach.

**Suggested Answer: C**

Community vote distribution



🗳️ 👤 **fightingpotato** 2 months, 2 weeks ago

**Selected Answer: C**

A confidentiality breach happens when unauthorized access to data occurs — even if the data hasn't been deleted, changed, or moved.  
upvoted 1 times

🗳️ 👤 **44d06fe** 3 months, 3 weeks ago

**Selected Answer: C**

Confidentiality breach  
upvoted 2 times

🗳️ 👤 **Ashwin123** 5 months, 2 weeks ago

**Selected Answer: C**

D can not be the answer as "everything seems to be in place" as per the scenario and Integrity Breach meaning possible alteration/destruction/manipulation of data  
upvoted 2 times

🗳️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: D**

It is definitely D and here's why it is not answer C. Confidentiality breach occurs when sensitive information is exposed to unauthorized individuals, either intentionally or accidentally. This scenario doesn't suggest that sensitive data is being exposed, but rather that unusual activity is happening on company files, which may point to a breach of data integrity.  
upvoted 2 times

🗳️ 👤 **7f814c6** 11 months ago

**Selected Answer: D**

D. Integrity Breach: An integrity breach involves unauthorized alterations to data, affecting its accuracy or completeness. Since Ben notices unusual activity and is concerned that something might be amiss with the company files, this could imply that the data might have been tampered with or altered in some way, affecting its integrity. Not C. A confidentiality breach involves unauthorized access to data, potentially exposing it to unauthorized parties. While Ben's concern might also involve unauthorized access, the description focuses more on unusual activity that could suggest tampering, which is more aligned with an integrity breach.  
upvoted 1 times

🗨️ 👤 **katizeti** 1 year, 5 months ago

Confidentiality Breach - A

upvoted 1 times

🗨️ 👤 **Cock** 1 year, 8 months ago

**Selected Answer: C**

A confidentiality breach involves unauthorized access to sensitive or private information, which matches the situation Ben is noticing unusual user activity on company files.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.

One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.

Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.

Going forward, what is the best way for IgNight to prepare its IT team to manage these kind of security events?

- A. Tabletop exercises.
- B. Update its data inventory.
- C. IT security awareness training.
- D. Share communications relating to scheduled maintenance.

**Suggested Answer: A**

*Community vote distribution*

A (82%)

C (18%)

🗳️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: A**

I agree that it is A as well. It's not C, because the IT security awareness training has been somewhat sent via email for a lookout.  
upvoted 1 times

🗳️ 👤 **7f814c6** 11 months ago

**Selected Answer: A**

These are simulated scenarios where team members work through potential security incidents in a controlled environment. Tabletop exercises help teams practice their response procedures, identify gaps in their plans, and improve coordination and decision-making during actual events. They are particularly useful for preparing teams to handle complex or unexpected security incidents.  
upvoted 1 times

🗳️ 👤 **VinL** 11 months ago

**Selected Answer: A**

Answer should be A so that all employees can understand what needs to be done during a security incident or data breach.  
upvoted 2 times

🗳️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: A**

Tabletop  
upvoted 1 times

🗳️ 👤 **DPRamone** 1 year, 4 months ago

**Selected Answer: A**

Tabletop exercise. Since he is obviously already aware that something is looking suspicious, the next step is a tabletop exercise to find out how to act on it.  
upvoted 2 times

🗳️ 👤 **katizeti** 1 year, 5 months ago

A. Tabletop exercises.  
upvoted 1 times

🗨️ 👤 **ET1857** 1 year, 8 months ago

**Selected Answer: A**

Answer is A

Look for the phrase -IT team to manage these kind of security events  
Its role based training and the closest option is tabletop exercise  
upvoted 2 times

🗨️ 👤 **ET1857** 1 year, 8 months ago

Answer is A

Look for the phrase -IT team to manage these kind of security events  
Its role based training and the closest option is tabletop exercise  
upvoted 1 times

🗨️ 👤 **Cock** 1 year, 8 months ago

**Selected Answer: C**

Security awareness training helps employees understand security risks, recognize suspicious activities, and take appropriate actions to protect the company's data and systems.  
upvoted 2 times

Which of the following is NOT typically a function of a Privacy Officer?

- A. Managing an organization's information security infrastructure.
- B. Serving as an interdepartmental liaison for privacy concerns.
- C. Monitoring an organization's compliance with privacy laws.
- D. Responding to information access requests from the public.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗳️ 👤 **Boerenkool** Highly Voted 🍌 1 year, 4 months ago

**Selected Answer: A**

Managing security is the responsibility of the security officer not the privacy officer  
upvoted 5 times

🗳️ 👤 **Ssourav** Most Recent 🕒 10 months, 3 weeks ago

**Selected Answer: A**

While Privacy Officers may work closely with IT and security teams, they typically do not directly manage the information security infrastructure. That task is usually the responsibility of an IT or security team. Privacy Officers focus on privacy regulations, policies, and procedures, ensuring that personal data is processed and stored in compliance with applicable laws.  
upvoted 2 times

🗳️ 👤 **DracoL** 1 year, 2 months ago

**Selected Answer: A**

I wonder if Examtopics really spend a little to double check on the answer and give a better response. A should be responsibilities of IT and CISO  
upvoted 3 times

🗳️ 👤 **FSampaio** 1 year, 3 months ago

Agreed, letter A is right. Subject Rights. Art. 15 GDPR. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information...  
upvoted 3 times

🗳️ 👤 **katizeti** 1 year, 4 months ago

I agree. A is a right answer  
upvoted 4 times

What is the main reason to begin with 3-5 key metrics during the program development process?

- A. To avoid undue financial costs.
- B. To keep the focus on the main organizational objectives.
- C. To minimize selective data use.
- D. To keep the process limited to as few people as possible.

**Suggested Answer: B**

*Community vote distribution*

B (100%)

  **humhain** 10 months, 3 weeks ago

**Selected Answer: B**



it can help to align the privacy program with the organization's vision, mission and goals, and to measure the progress and performance of the program against these objectives. By starting with a small number of key metrics, the program development process can avoid being overwhelmed or distracted by too many or irrelevant data points, and can prioritize and concentrate on the areas that matter most for the organization.

upvoted 1 times

  **carlosbui** 1 year, 1 month ago

should be B

upvoted 1 times

  **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

Starting with a limited number of key metrics allows an organization to maintain a clear direction and ensure that efforts align with its primary goals. As the program matures, additional metrics can be incorporated. However, beginning with too many metrics can dilute focus and make it harder to determine which activities are driving success.

upvoted 3 times

  **Adyyogi** 1 year, 5 months ago

B- because -..."As a basic business practice in the selection of metrics, the privacy professional should select three to five key privacy metrics that focus on the key organizational objectives. They can then assist other functions with other metrics that may have privacy implications."... CIPM Manual 2013/ pag70 .

upvoted 3 times

  **creativesyde** 1 year, 5 months ago

I think B is correct

upvoted 3 times

  **bilgecell** 1 year, 8 months ago

If you know why, please, share your comment. I didn't find answer at CIPM book.

upvoted 1 times



What is the main purpose of a privacy program audit?

- A. To mitigate the effects of a privacy breach.
- B. To justify a privacy department budget increase.
- C. To make decisions on privacy staff roles and responsibilities.
- D. To ensure the adequacy of data protection procedures.

**Suggested Answer:** D

*Community vote distribution*

D (100%)

 **Cock** 8 months, 1 week ago

**Selected Answer:** D

A privacy program audit is conducted to assess and validate that the organization's data protection procedures and practices are effective and in compliance with relevant regulations and policies.

upvoted 2 times

Under the General Data Protection Regulation (GDPR), when would a data subject have the right to require the erasure of his or her data without undue delay?

- A. When the data subject is a public authority.
- B. When the erasure is in the public interest.
- C. When the processing is carried out by automated means.
- D. When the data is no longer necessary for its original purpose.

**Suggested Answer: D**

Community vote distribution

D (100%)

FSampaio Highly Voted 1 year, 3 months ago

Letter D is right.  
upvoted 5 times

sham222 Highly Voted 1 year, 2 months ago

**Selected Answer: D**

D is correct.  
upvoted 5 times

carlosbui Most Recent 7 months, 3 weeks ago

should be D  
upvoted 1 times

Ssourav 10 months, 3 weeks ago

**Selected Answer: D**

When the data is no longer necessary for its original purpose. This is one of the conditions mentioned in Article 17 (1) (a) of the GDPR, commonly referred to as the "right to be forgotten."  
upvoted 3 times

emily0922 11 months ago

D is correct, Erasure is allowed when:

- data no longer needed for original purpose
- consent withdrawn and no other legal basis
- data subject objects to processing and no other legitimate basis
- legal obligation
- processing of personal info in relation to offer of info society service to a minor
- unlawful processing

upvoted 4 times

Adyyogi 11 months ago

D is correct  
upvoted 2 times

DracoL 1 year, 2 months ago

**Selected Answer: D**

D is correct  
upvoted 3 times

Boerenkool 1 year, 4 months ago

**Selected Answer: D**

Gdpr art 17, sect 1a  
upvoted 4 times

Larryqwe 1 year, 4 months ago

Should D i think.  
upvoted 4 times



What is the key factor that lays the foundation for all other elements of a privacy program?

- A. The applicable privacy regulations
- B. The structure of a privacy team
- C. A privacy mission statement
- D. A responsible internal stakeholder

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **sham222** Highly Voted 👍 1 year, 2 months ago

**Selected Answer:** C

C. A privacy mission statement  
upvoted 5 times

🗳️ 👤 **Ssourav** Most Recent 🕒 10 months, 3 weeks ago

**Selected Answer:** C

The mission statement sets the overall direction, purpose, and tone for the program, guiding subsequent actions, decisions, and priorities.

Additional reference : CIPM Official CBK 3rd Edition Section 2.2 "Define Privacy Program Scope"

upvoted 4 times

🗳️ 👤 **Alex951** 1 year, 1 month ago

**Selected Answer:** C

should be c  
upvoted 4 times

🗳️ 👤 **DracoL** 1 year, 2 months ago

**Selected Answer:** C

Should be C.  
upvoted 4 times

🗳️ 👤 **privacywarrior** 1 year, 2 months ago

**Selected Answer:** C

C is right  
upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

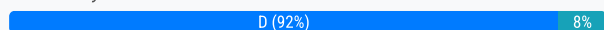
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

In consideration of the company's new initiatives, which of the following laws and regulations would be most appropriate for Albert to mention at the interview as a priority concern for the privacy team?

- A. Gramm-Leach-Bliley Act (GLBA)
- B. The General Data Protection Regulation (GDPR)
- C. The Telephone Consumer Protection Act (TCPA)
- D. Health Insurance Portability and Accountability Act (HIPAA)

**Suggested Answer: D**

Community vote distribution



**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: D**

Here's why I think it is D. Key word to look for is new initiative since that is what the question asks. Telemarketing is not a new initiative. This acquisition will likely trigger the need for HIPAA compliance but not saying that it would.

upvoted 1 times

**c4c7b78** 1 year ago

The context is US – nothing relates to the GDPR so B is not correct. GLBA is for banking services, so only C and D are applicable. Since the purchase of a medical supply company is still future (and there is not a clear indication of whether they will be sharing PI), it is not likely to be HIPAA. The most likely answer is C, since that is where they have challenges and 'flagrant disregard'.

upvoted 1 times

**humhain** 1 year, 4 months ago

**Selected Answer: D**

Health Insurance Portability and Accountability Act (HIPAA)

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: D**

Should be D

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: D**

HIPAA deals with the protection of medical records and other personal health information, which would be directly relevant if Treasure Box is entering the medical supply industry. This act mandates the safeguarding of personal health information and sets standards for the confidentiality, integrity, and availability of health records.

upvoted 2 times

🗨️ 👤 **Adyyogi** 1 year, 11 months ago

**Selected Answer: D**

-medical services - HIPAA- D

upvoted 2 times

🗨️ 👤 **Boats** 2 years ago

**Selected Answer: C**

They may or may not need protected health information for the new acquisition so D is a possibility. However, they do have a call center and have to deal with TCPA right now.

upvoted 1 times

🗨️ 👤 **DPRamone** 1 year, 4 months ago

B. "In consideration of the company's NEW initiatives"

upvoted 1 times

🗨️ 👤 **Alex951** 2 years, 1 month ago

**Selected Answer: D**

Should be HIPAA

upvoted 2 times

🗨️ 👤 **Boerenkool** 2 years, 4 months ago

**Selected Answer: D**

Hipaa applies to companies dealing with health data

upvoted 3 times

🗨️ 👤 **Larryqwe** 2 years, 4 months ago

Should be d HIPAA: acquiring a company dealing in health data

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

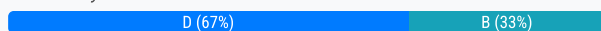
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

On which of the following topics does Albert most likely need additional knowledge?

- A. The role of privacy in retail companies
- B. The necessary maturity level of privacy programs
- C. The possibility of delegating responsibilities related to privacy
- D. The requirements for a managerial position with privacy protection duties

**Suggested Answer: C**

*Community vote distribution*



**fightingpotato** 2 months, 2 weeks ago

**Selected Answer: B**

Albert believes Treasure Box must meet the highest level of the AICPA/CICA Privacy Maturity Model (PMM), but not every company needs to be at the highest level.

upvoted 1 times

**katizeti** 11 months, 3 weeks ago

I think that he may need additional knowledge on the necessary maturity level of privacy programs - B.

upvoted 3 times

**carlosbui** 1 year, 1 month ago

should be B

upvoted 3 times

**Ssourav** 1 year, 4 months ago

**Selected Answer: D**

A. The role of privacy in retail companies - Albert has shown a good understanding of the importance of privacy in Treasure Box, especially concerning customer data.

B. The necessary maturity level of privacy programs - Albert is knowledgeable about the AICPA/CICA Privacy Maturity Model (PMM) and has identified gaps in the company's current maturity level.

C. The possibility of delegating responsibilities related to privacy - The scenario doesn't provide direct information on Albert's knowledge or lack thereof regarding delegation.

D. The requirements for a managerial position with privacy protection duties - Albert, despite his years at the company, has been repeatedly overlooked for managerial roles. This suggests that while he might be knowledgeable about privacy concerns, he might not be well-acquainted with what is required to manage such duties at the managerial level.

Considering the information given, D. The requirements for a managerial position with privacy protection duties still seems like the most appropriate answer.

upvoted 1 times

🗨️ 👤 **emily0922** 1 year, 5 months ago

Should be B too, a company does not need to reach the highest level of a maturity model to be compliant/have good practices

upvoted 3 times

🗨️ 👤 **Adyyogi** 1 year, 5 months ago

**Selected Answer: D**

- d - because he has no previous experience as a manager or privacy specialist

upvoted 1 times

🗨️ 👤 **Boerenkool** 1 year, 10 months ago

Why not b?

upvoted 2 times



## SCENARIO -

Please use the following to answer the next question:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

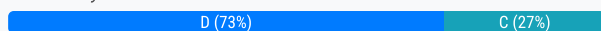
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

Based on Albert's observations, executive leadership should most likely pay closer attention to what?

- A. Awareness campaigns with confusing information
- B. Obsolete data processing systems
- C. Outdated security frameworks
- D. Potential in-house threats

**Suggested Answer: D**

*Community vote distribution*



**manjo23** 8 months ago

**Selected Answer: C**

The paragraph mentions:

he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

Because this is an executive leadership issue!

upvoted 3 times

**humhain** 10 months, 1 week ago

**Selected Answer: D**

Potential in-house threats

upvoted 1 times

**katzeti** 11 months, 3 weeks ago

Executive leadership should most likely pay closer attention to outdated security frameworks. Albert has identified lapses in the company's privacy program and plans to make executives aware of these lapses during his interview.

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: D**

the most concerning observation Albert made relates to the internal structure of the company, specifically the high turnover and the potential that these new and potentially discontented employees might not adhere to company procedures. This can present potential in-house threats. Therefore, the answer is: D.

upvoted 3 times

🗨️ 👤 **Adyyogi** 1 year, 5 months ago

**Selected Answer: D**

D- because... "Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be a flagrant disregard for company procedures."

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

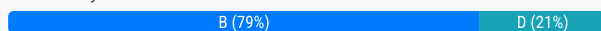
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

Based on Albert's observations regarding recent security incidents, which of the following should he suggest as a priority for Treasure Box?

- A. Appointing an internal ombudsman to address employee complaints regarding hours and pay.
- B. Using a third-party auditor to address privacy protection issues not recognized by the prior internal audits.
- C. Working with the Human Resources department to make screening procedures for potential employees more rigorous.
- D. Evaluating the company's ability to handle personal health information if the plan to acquire the medical supply company goes forward

**Suggested Answer: B**

Community vote distribution



**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: B**

B is correct. D isn't correct since the company did not go through with it yet. If it did, then different story.  
upvoted 2 times

**MaritzTee** 7 months, 1 week ago

**Selected Answer: B**

This recommendation directly addresses the security incidents by bringing in an external perspective to identify and rectify any privacy protection issues that may have been overlooked during internal audits. This can help restore trust and improve the company's security measures, ultimately safeguarding customer and employee personal data more effectively.  
upvoted 3 times

**thecheaterz** 7 months, 3 weeks ago

**Selected Answer: B**

The question is talking about recent security incidents. Not the potential healthcare acquisition  
upvoted 3 times

**humhain** 10 months, 1 week ago



**Selected Answer: D**

Evaluating the company's ability to handle personal health information if the plan to acquire the medical supply company goes forward  
upvoted 1 times

  **DPRamone** 10 months, 1 week ago

**Selected Answer: B**

A third party audit could include the capability of handling PHI, thus constituting a more comprehensive solution than just going for D.  
upvoted 2 times

  **katizeti** 11 months, 3 weeks ago

In my opinion B

upvoted 1 times

  **carlosbui** 1 year, 1 month ago

should be D

upvoted 1 times

  **Ssourav** 1 year, 4 months ago

**Selected Answer: D**

it would be imperative for Treasure Box to ensure its capability to handle personal health information securely and in compliance with relevant regulations. The acquisition of a medical supply company introduces new potential risks and challenges, especially around the handling of sensitive health data.

Therefore, evaluating the company's capacity to handle this data securely (Option D) would be a proactive approach in ensuring they don't further erode trust or face potential regulatory backlash.

upvoted 2 times

  **Adyyogi** 1 year, 5 months ago

**Selected Answer: B**

B- because the subject is : Albert's observations regarding recent security incidents.."

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

What is one important factor that Albert fails to consider regarding Treasure Box's response to their recent security incident?

- A. Who has access to the data
- B. What the nature of the data is
- C. How data at the company is collected
- D. How long data at the company is kept

**Suggested Answer: B**

*Community vote distribution*



B (100%)

  **humhain** 10 months, 1 week ago

**Selected Answer: B**


This answer is an important factor that Albert fails to consider, as it can affect the legal and ethical obligations and implications of the company's response to the security incident, as well as the potential impact and harm to the individuals whose data is involved. The nature of the data refers to the type, category, sensitivity and value of the data that is collected, processed and stored by the company, such as personal, financial, health, biometric or behavioral data. Depending on the nature of the data, the company may have different requirements or restrictions for notifying, reporting or disclosing the security incident to the relevant authorities, customers, partners or stakeholders, as well as for mitigating or compensating the effects of the incident.

upvoted 2 times

  **carlosbui** 1 year, 1 month ago

should be B

upvoted 1 times

  **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

it seems that Albert is focused on various other aspects of the company's operations and security, but the specific nature of the data affected by the security incidents isn't mentioned as something he's considering. Understanding the type of data involved (e.g., financial, health, personal identifiers) is critical because it can influence the severity of an incident, its regulatory implications, and the potential consequences for affected individuals.

upvoted 2 times

🗨️ 👤 **Adyyogi** 1 year, 5 months ago

**Selected Answer: B**

B- based on the information provided

upvoted 2 times

🗨️ 👤 **Larryqwe** 1 year, 9 months ago

**Selected Answer: B**

More info on the type of security breach is needed.

upvoted 4 times

🗨️ 👤 **Boerenkool** 1 year, 10 months ago

**Selected Answer: B**

If no personal identifiable information was involved, reporting to the public is not required

upvoted 3 times

🗨️ 👤 **Larryqwe** 1 year, 10 months ago

Not a lot of info about security incident is given. Hard to answer this question

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.

Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her "I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?" He has also told her that he works with a number of small companies that help him get projects completed in a hurry. "We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have."

In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team "didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end." Penny is concerned that these issues will compromise Ace Space's privacy and data protection.

Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data "shake up". Her mission is to cultivate a strong privacy culture within the company.

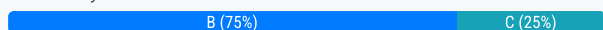
Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.

To help Penny and her CEO with their objectives, what would be the most helpful approach to address her IT concerns?

- A. Roll out an encryption policy
- B. Undertake a tabletop exercise
- C. Ensure inventory of IT assets is maintained
- D. Host a town hall discussion for all IT employees

**Suggested Answer: B**

Community vote distribution



🗳️ 👤 **c4c7b78** 1 year ago

**Selected Answer: C**

A is the least likely to have an effect. A tabletop exercise will only be effective if there are proper procedures defined ("we don't know what to do or who should do what"). As a manager I would lean toward D but the most likely correct answer is C.

upvoted 1 times

🗳️ 👤 **MaritzTee** 1 year, 1 month ago

**Selected Answer: B**

This approach will help the IT team simulate a real-world scenario, such as a data breach or phishing attack, and practice their response in a controlled environment. It will highlight gaps in their knowledge, response procedures, and coordination, enabling them to improve their readiness for actual incidents. Given the previous issues with phishing attacks and the loss of encrypted USB keys, this practical exercise will be invaluable in ensuring the IT team knows what to do and who should do what in case of future incidents.

While the other options are beneficial, they do not directly address the immediate need for the IT team to be prepared for and effectively respond to security incidents, which is a critical concern identified by Penny.

upvoted 2 times

🗳️ 👤 **DPRamone** 1 year, 4 months ago

**Selected Answer: C**

Everything starts with an up-to-date asset inventory and classification. You can't protect what you don't know you have.



upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 10 months ago

**Selected Answer: B**

Should be B

upvoted 2 times

  **Ssourav** 1 year, 10 months ago

**Selected Answer: B**

given the information provided in the scenario, undertaking a tabletop exercise would be the most effective approach for several reasons:

Identifying Response Gaps: A tabletop exercise allows a company to walk through a hypothetical, but realistic, situation to determine how they would respond. This can help highlight any gaps in the response process.

Training: Since Penny's IT colleague mentioned they "didn't know what to do or who should do what" during a previous phishing attack, a tabletop exercise would serve as an effective training tool, giving the team clarity on roles, responsibilities, and actions to take during an incident.

Building Confidence: By running through these simulations, the IT team can become more confident in their abilities to handle real-world situations when they arise.

While the other options are valid in their own contexts, given the specific concerns Penny has learned about Ace Space's IT practices, the tabletop exercise directly addresses the identified issues and provides the most immediate benefits.

upvoted 2 times

  **emily0922** 1 year, 11 months ago

I suggest B

upvoted 1 times



## SCENARIO -

Please use the following to answer the next question:

For 15 years, Albert has worked at Treasure Box – a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.

He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.

For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.

Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.

In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public is unaware of, although Albert does not know the details. He believes the company's insistence on keeping the incident a secret could be a further detriment to its reputation. One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail.

In addition to his suggestions for improvement, Albert believes that his knowledge of the company's recent business maneuvers will also impress the interviewers. For example, Albert is aware of the company's intention to acquire a medical supply company in the coming weeks.

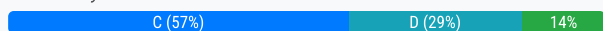
With his forward thinking, Albert hopes to convince the managers who will be interviewing him that he is right for the job.

The company may start to earn back the trust of its customer base by following Albert's suggestion regarding which handling procedure?

- A. Access
- B. Correction
- C. Escalation
- D. Data Integrity

**Suggested Answer: C**

*Community vote distribution*



**fightingpotato** 3 months, 1 week ago

**Selected Answer: A**

Given that Albert's suggestion focuses on improving customer communication channels—such as a toll-free number and a more efficient procedure for responding to customer concerns—Access (A) might be the best choice.

upvoted 1 times

**humhain** 10 months, 1 week ago

**Selected Answer: D**

Data integrity

upvoted 2 times

**carlosbui** 1 year, 1 month ago

should be C

upvoted 1 times

**Ssourav** 1 year, 4 months ago

**Selected Answer: C**

The option that best aligns with Albert's suggestion to directly address customer concerns is "C. Escalation." This option implies that customer concerns would be promptly escalated to higher management or the appropriate department, ensuring they're addressed efficiently and effectively.

upvoted 2 times

  **Adyyogi** 1 year, 5 months ago

**Selected Answer: C**

c- mostly because: "One further way that Albert wants to help Treasure Box regain its stature is by creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail..."

upvoted 2 times


"Collection", "access" and "destruction" are aspects of what privacy management process?

- A. The data governance strategy
- B. The breach response plan
- C. The metric life cycle
- D. The business case

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: A**

Correct answer is A.

upvoted 1 times

What does it mean to “rationalize” data protection requirements?

- A. Evaluate the costs and risks of applicable laws and regulations and address those that have the greatest penalties
- B. Look for overlaps in laws and regulations from which a common solution can be developed
- C. Determine where laws and regulations are redundant in order to eliminate some from requiring compliance
- D. Address the less stringent laws and regulations, and inform stakeholders why they are applicable

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: B**

I agree that it is B. C is automatically eliminated since you can't just get rid of laws and regulations.

upvoted 1 times

🗳️ 👤 **Ssourav** 10 months, 3 weeks ago

**Selected Answer: B**

When dealing with multiple laws and regulations, particularly in a global environment, there can be overlapping or similar requirements. Rationalizing these requirements involves identifying commonalities or overlaps so that a unified approach can be developed to address multiple requirements at once. This ensures efficiency and coherence in compliance efforts.

upvoted 2 times

🗳️ 👤 **Adyyogi** 11 months ago

b- because: "One option is to rationalize requirements, which essentially means implementing a solution that materially addresses them. This activity is made simpler by several factors. First, at a high level, most data privacy legislation imposes many of the same types of obligations on regulated entities, and much of this regulation requires entities to offer similar types of rights to individuals.."cipm manual,third ed, cap.2.5.3 Rationalizing Requirements

upvoted 3 times

🗳️ 👤 **DracoL** 1 year, 2 months ago

**Selected Answer: B**

B make more sense and the most strict regulatory requirement

upvoted 2 times

🗳️ 👤 **Luton** 1 year, 2 months ago

Should be B

upvoted 3 times

🗳️ 👤 **sham222** 1 year, 2 months ago

**Selected Answer: B**

B is the right answer

upvoted 4 times

🗳️ 👤 **Larryqwe** 1 year, 3 months ago

**Selected Answer: B**

You'll always need compliance.even when there's redundancy

upvoted 2 times

Which term describes a piece of personal data that alone may not identify an individual?

- A. Unbundled data
- B. A singularity
- C. Non-aggregated infopoint
- D. A single attribute

**Suggested Answer:** D

Community vote distribution

D (100%)

🗳️ 👤 **humhain** 10 months, 1 week ago

**Selected Answer: D**

A single attribute

upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 1 month ago

should be D

upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: D**

A single attribute refers to a piece of information or data about an individual that, on its own, may not necessarily identify them. However, when combined with other attributes, it can contribute to uniquely identifying an individual.

upvoted 2 times

🗳️ 👤 **emily0922** 1 year, 4 months ago

I suggest D

upvoted 1 times

🗳️ 👤 **Adyyogi** 1 year, 5 months ago

**Selected Answer: D**

D. the same explanation .." A single attribute describes a piece of personal data that alone may not identify an individual. "

upvoted 2 times

🗳️ 👤 **sham222** 1 year, 8 months ago

**Selected Answer: D**

D. A single attribute describes a piece of personal data that alone may not identify an individual.

Personal data refers to any information relating to an identified or identifiable natural person. A single attribute, such as someone's birthdate or postal code, may not be sufficient to identify a specific individual on its own, but it can be combined with other data points to create a more complete picture of the person's identity.

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud."

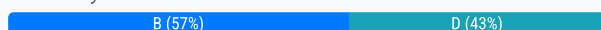
You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.

After conducting research, you discover a primary data protection issue with cloud computing. Which of the following should be your biggest concern?

- A. An open programming model that results in easy access
- B. An unwillingness of cloud vendor to provide security information
- C. A lack of vendors in the cloud computing market
- D. A reduced resilience of data structures that may lead to data loss.

**Suggested Answer: B**

Community vote distribution



**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: D**

The scenario does not explicitly mention the cloud vendor's unwillingness to provide security information, so B is automatically out. I can't think of a scenario where the cloud provider wouldn't give you security info?

The correct answer, based on the information in the scenario, would likely be D. A reduced resilience of data structures that may lead to data loss.  
upvoted 1 times

**MaritzTee** 7 months, 1 week ago

**Selected Answer: B**

In cloud computing, the level of security and privacy controls implemented by the cloud provider is crucial. If the vendor is unwilling to provide detailed information about their security practices, it raises a significant red flag. You need to understand how your data will be protected, what measures are in place to prevent unauthorized access, and how the vendor will handle potential breaches. Transparency from the cloud provider is essential to ensure they meet your organization's security and privacy requirements.

The other options, while relevant, do not address the core issue of needing clear and reliable information about the vendor's security practices, which is fundamental to protecting customer data.



upvoted 2 times

**DPRamone** 10 months, 1 week ago

**Selected Answer: D**



D makes sense since I have no idea what an open programming model (A) is and neither does Google. Your average cloud provider lists an entire page of security and other certifications, and although they generally won't consent to an audit, they are quite forthcoming with their security measures.

upvoted 1 times

  **katizeti** 11 months, 3 weeks ago

In my opinion A. Cloud computing involves the sharing of resources and data across multiple users and systems, which can create security vulnerabilities if not properly secured. An open programming model can make it easier for attackers to exploit these vulnerabilities and gain unauthorized access to sensitive data. The primary data protection issue with cloud computing that should be of biggest concern is an open programming model that results in easy access.

upvoted 1 times

  **Cock** 1 year, 2 months ago

**Selected Answer: D**

D, Moving customer data to a data cloud introduces the risk of data loss if the data structures used by the cloud service provider are not resilient enough. Data loss can occur due to various reasons such as hardware failure, software bugs, natural disasters, or human errors. If the data structures in the cloud are not designed to handle such scenarios effectively, it could lead to the loss of critical customer data.

upvoted 1 times


  **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

B. An unwillingness of cloud vendor to provide security information.

This is because if the cloud vendor is unwilling to provide security information, it raises concerns about the measures they have in place to protect the data and the organization's ability to assess and ensure the security of its customers' data.

upvoted 2 times

  **emily0922** 1 year, 4 months ago

I suggest A, it is most linked to the CIA triad

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud."

You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.

What is the best way to prevent the Finnish vendor from transferring data to another party?

- A. Restrict the vendor to using company security controls
- B. Offer company resources to assist with the processing
- C. Include transfer prohibitions in the vendor contract
- D. Lock the data down in its current location

**Suggested Answer: C**

*Community vote distribution*

C (100%)

Privacy2024 6 months, 2 weeks ago

**Selected Answer: C**

I also agree with C.

upvoted 1 times

Ssourav 10 months ago

**Selected Answer: C**

C. Include transfer prohibitions in the vendor contract.

By explicitly stating the terms and conditions regarding data transfers in the contract, the vendor would be legally bound to adhere to those stipulations.

upvoted 2 times



## SCENARIO -

Please use the following to answer the next question:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud."

You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.

What process can best answer your questions about the vendor's data security safeguards?

- A. A second-party of supplier audit
- B. A reference check with other clients
- C. A table top demonstration of a potential threat
- D. A public records search for earlier legal violations

**Suggested Answer: A**

*Community vote distribution*

A (100%)

Privacy2024 6 months, 2 weeks ago

**Selected Answer: A**

Answer is definitely A.

upvoted 1 times

carlosbui 7 months, 3 weeks ago

should be A

upvoted 2 times

Ssourav 10 months ago

**Selected Answer: A**

A. A second-party or supplier audit.

This process allows for a direct examination and evaluation of the vendor's security measures, ensuring they meet the required standards and expectations.

upvoted 1 times

Gh789 10 months, 2 weeks ago

A - auditing the vendor (2nd party audit) can help to resolve any queries about security safeguards at vendor side

upvoted 2 times

SachPP 12 months ago

why not A - a second party audit

upvoted 3 times

## SCENARIO -

Please use the following to answer the next question:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the "misunderstanding" has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. "The good news," he says, "is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud."

You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.

What is the best way for your vendor to be clear about the Society's breach notification expectations?

- A. Include notification provisions in the vendor contract
- B. Arrange regular telephone check-ins reviewing expectations
- C. Send a memorandum of understanding on breach notification
- D. Email the regulations that require breach notifications

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: A**

I agree that it's answer A.

upvoted 1 times

  **Ssourav** 10 months ago

**Selected Answer: A**

A. Include notification provisions in the vendor contract.

A contractual provision will explicitly detail the requirements, responsibilities, and timelines related to breach notifications, providing a legally enforceable framework for the vendor's actions in the event of a breach.

upvoted 2 times

What is the function of the privacy operational life cycle?

- A. It establishes initial plans for privacy protection and implementation
- B. It allows the organization to respond to ever-changing privacy demands
- C. It ensures that outdated privacy policies are retired on a set schedule
- D. It allows privacy policies to mature to a fixed form

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗳️ **alaaz** 7 months, 2 weeks ago

**Selected Answer: B**

B is the correct answer

upvoted 1 times

🗳️ **humhain** 1 year, 4 months ago

**Selected Answer: B**

B. It allows the organization to respond to ever-changing privacy demands

upvoted 1 times

🗳️ **carlosbui** 1 year, 7 months ago

should be B

upvoted 1 times

🗳️ **Ssourav** 1 year, 10 months ago

**Selected Answer: B**

B. It allows the organization to respond to ever-changing privacy demands.

The privacy operational life cycle ensures that an organization can continually assess, implement, maintain, and revise its privacy strategies and practices in response to evolving organizational needs, technological changes, and regulatory landscapes. This cyclical approach helps organizations stay adaptive and up-to-date in the dynamic field of privacy.

upvoted 1 times

🗳️ **emily0922** 1 year, 11 months ago

I propose B

upvoted 1 times

🗳️ **mgmferreira** 2 years, 1 month ago

**Selected Answer: B**

Letra B

upvoted 1 times

Which is the best way to view an organization's privacy framework?

- A. As an industry benchmark that can apply to many organizations
- B. As a fixed structure that directs changes in the organization
- C. As an aspirational goal that improves the organization
- D. As a living structure that aligns to changes in the organization

**Suggested Answer:** D

*Community vote distribution*

D (100%)

🗳️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer:** D

I agree with D.

upvoted 1 times

🗳️ 👤 **carlosbui** 7 months, 3 weeks ago

should be D

upvoted 2 times

🗳️ 👤 **Ssourav** 10 months ago

**Selected Answer:** D

D. As a living structure that aligns to changes in the organization.

A privacy framework should be adaptable and responsive to the evolving needs of the organization, technological advancements, regulatory changes, and emerging risks. By treating it as a "living structure," organizations can ensure that their privacy practices remain relevant and effective over time.

upvoted 3 times

🗳️ 👤 **emily0922** 11 months ago

Should be D

upvoted 1 times

🗳️ 👤 **mgmferreira** 1 year, 1 month ago

**Selected Answer:** D

Letra D

upvoted 1 times

An organization is establishing a mission statement for its privacy program. Which of the following statements would be the best to use?

- A. This privacy program encourages cross-organizational collaboration which will stop all data breaches
- B. Our organization was founded in 2054 to reduce the chance of a future disaster like the one that occurred ten years ago. All individuals from our area of the country should be concerned about a future disaster. However, with our privacy program, they should not be concerned about the misuse of their information.
- C. The goal of the privacy program is to protect the privacy of all individuals who support our organization. To meet this goal, we must work to comply with all applicable privacy laws.
- D. In the next 20 years, our privacy program should be able to eliminate 80% of our current breaches. To do this, everyone in our organization must complete our annual privacy training course and all personally identifiable information must be inventoried.

**Suggested Answer:** C

*Community vote distribution*

C (100%)

🗨️ 👤 **Ssourav** 10 months ago

**Selected Answer: C**

The best mission statement for a privacy program is C.

This statement is clear, concise, and actionable. It states the organization's goal of protecting the privacy of its stakeholders, and it identifies the specific steps that will be taken to achieve that goal.

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will: Send an enrollment invitation to everyone the day after the contract is signed.

Enroll someone with just their first name and the last-4 of their national identifier.

Monitor each enrollee's credit for two years from the date of enrollment.

Send a monthly email with their credit rating and offers for credit-related services at market rates.

Charge your company 20% of the cost of any credit restoration.

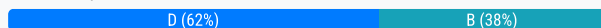
You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

Which of the following elements of the incident did you adequately determine?

- A. The nature of the data elements impacted
- B. The likelihood the incident may lead to harm
- C. The likelihood that the information is accessible and usable
- D. The number of individuals whose information was affected

**Suggested Answer: D**

*Community vote distribution*



**0ef35ef** 6 months, 1 week ago

**Selected Answer: D**

I might be missing something but the text states that "the vendor has lost control of the data." The parties never seem to clarify what that means exactly. They just go into action mode. Therefore, I would say that B is not correct but they did indeed know the exact number of individuals affected. upvoted 2 times

**Vinz\_** 6 months, 1 week ago

**Selected Answer: D**

The correct answer is D, since the number of individuals was exactly determined.

The answer B is wrong: the likelihood the incident may lead to harm was not adequately determined, in fact "shortly after postcards were sent, data

was on a server that was stolen".

upvoted 1 times

🗨️ 👤 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: D**

Answer is D. Watch out for keywords. Which of the following elements of the incident did you adequately determine. Adequately means that you pretty much got right. So that would be the number of affected individuals.

upvoted 2 times

🗨️ 👤 **7f814c6** 11 months ago

**Selected Answer: B**

The scenario highlights that the data was related to a sensitive context—healthcare information—which could lead to significant harm if exposed. Although you confirmed the exact number of affected individuals (2000), the assessment of the likelihood of harm due to the exposure of sensitive data is crucial and was not addressed with as much clarity.

The other elements, such as the exact number of affected individuals, were determined accurately, but the potential for harm from such sensitive data, particularly given the theft of the server, is a critical aspect that requires thorough evaluation.

upvoted 1 times

🗨️ 👤 **MaritzTee** 1 year, 1 month ago

**Selected Answer: D**

The scenario explicitly states that exactly 2000 individuals were surveyed, and it was confirmed that these surveys were the ones impacted by the vendor's failure to encrypt the data. This clear identification and quantification of the affected individuals were adequately determined and used in the notification process.

The other elements, while important, were not addressed or resolved with the same clarity and certainty as the number of affected individuals.

upvoted 1 times

🗨️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: B**

I think B because the information was related to an infectious disease questionnaire which could be classed as sensitive data and cause potential harm. The 2000 names is irrelevant and there could be more data on the server.

upvoted 2 times

🗨️ 👤 **DPRamone** 1 year, 4 months ago

**Selected Answer: B**

The server was stolen. Who says the DB with the 2k individuals was the only resource affected ?

upvoted 2 times

🗨️ 👤 **katizeti** 1 year, 5 months ago

Seems that D is correct.

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: D**

D. The number of individuals whose information was affected

The scenario explicitly mentions that exactly 2000 individuals were affected by the vendor's oversight. The other elements, while touched upon to varying extents, were not as definitively determined as the exact number of individuals affected.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will: Send an enrollment invitation to everyone the day after the contract is signed.

Enroll someone with just their first name and the last-4 of their national identifier.

Monitor each enrollee's credit for two years from the date of enrollment.

Send a monthly email with their credit rating and offers for credit-related services at market rates.

Charge your company 20% of the cost of any credit restoration.

You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

Regarding the notification, which of the following would be the greatest concern?

- A. Informing the affected individuals that data from other individuals may have also been affected.
- B. Collecting more personally identifiable information than necessary to provide updates to the affected individuals.
- C. Using a postcard with the logo of the vendor who make the mistake instead of your company's logo.
- D. Trusting a vendor to send out a notice when they already failed once by not encrypting the database.

**Suggested Answer: B**

Community vote distribution

B (100%)

 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: B**

It is B. The notification asks individuals to provide their name, email address, and month and year of birth in order to sign up for email notifications. This raises a serious concern because collecting additional personal information beyond what is necessary for providing updates can be considered an unnecessary privacy risk. The original breach involved unauthorized access to personal healthcare data, so asking for more information may create a new risk of exposure and also be seen as an overreach, making this the greatest concern.

upvoted 2 times

 **katizeti** 11 months, 3 weeks ago

I think that D is correct



upvoted 1 times

  **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

B. Collecting more personally identifiable information than necessary to provide updates to the affected individuals.

The notification asked individuals to provide their name, email address, and month and year of birth after watching an advertisement. Given that the incident revolves around a breach of privacy, it's problematic to collect more data than absolutely necessary, potentially putting individuals at further risk and compromising trust.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will: Send an enrollment invitation to everyone the day after the contract is signed.

Enroll someone with just their first name and the last-4 of their national identifier.

Monitor each enrollee's credit for two years from the date of enrollment.

Send a monthly email with their credit rating and offers for credit-related services at market rates.

Charge your company 20% of the cost of any credit restoration.

You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

What is the most concerning limitation of the incident-response council?

- A. You convened it to diffuse blame
- B. The council has an overabundance of attorneys
- C. It takes eight hours of emails to come to a decision
- D. The leader just joined the company as a consultant

**Suggested Answer: A**

Community vote distribution



**Vinz\_** 6 months, 1 week ago

**Selected Answer: D**

Imagine joining a company and on the first day you lead a data breach incident response. I mean, you don't even remember which desk is yours..  
upvoted 1 times

**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: C**

In a data breach or privacy incident, time is critical. The faster you can assess the situation, determine the necessary actions, and communicate with affected parties, the better you can mitigate the potential damage. Waiting 8 hours to come to a decision could mean that important actions—such as

notifying affected individuals, securing systems, or stopping further data leaks—are delayed. This delay can increase the risk of harm to individuals and damage the company's reputation. Overall, this is limiting. A would definitely not be the right answer in this case.

upvoted 2 times

🗨️ 👤 **7f814c6** 11 months ago

**Selected Answer: A**

This is the most critical issue because it suggests that the council's purpose was more about assigning responsibility than effectively addressing the incident. Effective incident response should focus on resolving the issue and mitigating its impact rather than deflecting blame. The other concerns, while relevant, such as the new consultant's unfamiliarity with the organization or the lengthy decision-making process, are secondary to the fundamental issue of focusing on blame rather than resolution.

upvoted 2 times

🗨️ 👤 **MaritzTee** 1 year, 1 month ago

**Selected Answer: D**

The fact that the leader of the incident-response council just joined the company as a consultant indicates a potential lack of familiarity with the company's internal processes, culture, and protocols. This lack of experience within the organization could hinder their ability to effectively lead the incident-response efforts, make informed decisions, and navigate the complexities of the situation. It may also delay or impede the resolution of the incident, especially if the consultant is not familiar with the company's privacy policies and regulatory requirements.

While the other options may also present concerns, such as an overabundance of attorneys or lengthy decision-making processes, the presence of a newly appointed leader who lacks familiarity with the organization's operations poses a more immediate and significant risk to the incident-response process.

upvoted 2 times

🗨️ 👤 **thecheaterz** 1 year, 1 month ago

**Selected Answer: C**

A is not a limitation. C makes the most sense

upvoted 2 times

🗨️ 👤 **katizeti** 1 year, 5 months ago

C. It takes eight hours of emails to come to a decision.

upvoted 2 times

🗨️ 👤 **Ssourav** 1 year, 10 months ago

**Selected Answer: A**

A. You convened it to diffuse blame.

Using a council simply to diffuse blame rather than taking constructive actions and ensuring that the best decisions are made in the interest of the affected individuals and the organization is problematic. Effective incident response should be focused on rectifying the situation and protecting affected parties, not on avoiding responsibility.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will:

Send an enrollment invitation to everyone the day after the contract is signed.

Enroll someone with just their first name and the last-4 of their national identifier.

Monitor each enrollee's credit for two years from the date of enrollment.

Send a monthly email with their credit rating and offers for credit-related services at market rates.

Charge your company 20% of the cost of any credit restoration.

You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

Regarding the credit monitoring, which of the following would be the greatest concern?

- A. The vendor's representative does not have enough experience
- B. Signing a contract with CRUDLOK which lasts longer than one year
- C. The company did not collect enough identifiers to monitor one's credit
- D. You are going to notify affected individuals via a letter followed by an email

**Suggested Answer: C**

*Community vote distribution*


C (100%)

 **Privacy2024** 6 months, 2 weeks ago

**Selected Answer: C**

C makes total sense. If the monitoring service is only using the last four digits of the SSN/national identifier, it likely won't be able to identify the individual reliably in credit databases. This could lead to incomplete or failed credit monitoring, leaving individuals vulnerable to fraud without adequate protection.

upvoted 2 times

 **thecheaterz** 7 months, 3 weeks ago

**Selected Answer: C**

C makes sense

upvoted 1 times

🗨️ 👤 **katizeti** 11 months, 3 weeks ago

Maybe B?

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: C**

C. The company did not collect enough identifiers to monitor one's credit.

Monitoring someone's credit with just their first name and the last-4 of their national identifier is a significant limitation and could lead to inaccuracies or gaps in the monitoring process. Ensuring that there is sufficient data to accurately and effectively monitor an individual's credit is crucial for the service to be meaningful and protective.

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

You lead the privacy office for a company that handles information from individuals living in several countries throughout Europe and the Americas. You begin that morning's privacy review when a contracts officer sends you a message asking for a phone call. The message lacks clarity and detail, but you presume that data was lost.

When you contact the contracts officer, he tells you that he received a letter in the mail from a vendor stating that the vendor improperly shared information about your customers. He called the vendor and confirmed that your company recently surveyed exactly 2000 individuals about their most recent healthcare experience and sent those surveys to the vendor to transcribe it into a database, but the vendor forgot to encrypt the database as promised in the contract. As a result, the vendor has lost control of the data.

The vendor is extremely apologetic and offers to take responsibility for sending out the notifications. They tell you they set aside 2000 stamped postcards because that should reduce the time it takes to get the notice in the mail. One side is limited to their logo, but the other side is blank and they will accept whatever you want to write. You put their offer on hold and begin to develop the text around the space constraints. You are content to let the vendor's logo be associated with the notification.

The notification explains that your company recently hired a vendor to store information about their most recent experience at St. Sebastian Hospital's Clinic for Infectious Diseases. The vendor did not encrypt the information and no longer has control of it. All 2000 affected individuals are invited to sign-up for email notifications about their information. They simply need to go to your company's website and watch a quick advertisement, then provide their name, email address, and month and year of birth.

You email the incident-response council for their buy-in before 9 a.m. If anything goes wrong in this situation, you want to diffuse the blame across your colleagues. Over the next eight hours, everyone emails their comments back and forth. The consultant who leads the incident-response team notes that it is his first day with the company, but he has been in other industries for 45 years and will do his best. One of the three lawyers on the council causes the conversation to veer off course, but it eventually gets back on track. At the end of the day, they vote to proceed with the notification you wrote and use the vendor's postcards.

Shortly after the vendor mails the postcards, you learn the data was on a server that was stolen, and make the decision to have your company offer credit monitoring services. A quick internet search finds a credit monitoring company with a convincing name: Credit Under Lock and Key (CRUDLOK). Your sales rep has never handled a contract for 2000 people, but develops a proposal in about a day which says CRUDLOK will: Send an enrollment invitation to everyone the day after the contract is signed.

Enroll someone with just their first name and the last-4 of their national identifier.

Monitor each enrollee's credit for two years from the date of enrollment.

Send a monthly email with their credit rating and offers for credit-related services at market rates.

Charge your company 20% of the cost of any credit restoration.

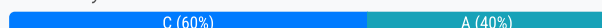
You execute the contract and the enrollment invitations are emailed to the 2000 individuals. Three days later you sit down and document all that went well and all that could have gone better. You put it in a file to reference the next time an incident occurs.

Which of the following was done CORRECTLY during the above incident?

- A. The process by which affected individuals sign up for email notifications
- B. Your assessment of which credit monitoring company you should hire
- C. The speed at which you sat down to reflect and document the incident
- D. Finding a vendor who will offer the affected individuals additional services

**Suggested Answer: C**

*Community vote distribution*



**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: A**

The process by which affected individuals sign up for email notifications: From a privacy management standpoint, ensuring that affected individuals are promptly notified and provided with the means to access further communication (e.g., email notifications) is a fundamental aspect of managing privacy incidents. Although the process used here is not ideal (asking individuals to watch an advertisement to sign up), it still provides a clear method for individuals to take action. It's important to prioritize transparent and accessible communication with affected individuals.

C. The speed at which you sat down to reflect and document the incident: While reflecting and documenting the incident quickly is important, from a privacy management perspective, the immediate focus should typically be on communicating with the affected individuals and managing the breach.

effectively. This reflects the core principles of managing a privacy incident, as outlined in the CIPM framework, where your first priority is usually to minimize harm and provide transparency to affected individuals.

upvoted 2 times

🗨️ 👤 **MaritzTee** 7 months, 1 week ago

**Selected Answer: C**

C. The speed at which you sat down to reflect and document the incident

The scenario describes that three days after the enrollment invitations were emailed to the 2000 individuals, you took the time to document all that went well and all that could have gone better. This prompt reflection and documentation are crucial for learning from the incident and improving future responses, indicating that the speed at which this was done was correct.

upvoted 1 times

🗨️ 👤 **katizeti** 11 months, 3 weeks ago

C could be ok

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: C**

C. The speed at which you sat down to reflect and document the incident.

After an incident, it's vital to reflect on the situation, analyze what happened, what was done well, and what could be improved. This reflection should be done as soon as possible while the events are still fresh. By documenting the incident and the response shortly after its conclusion, you ensure that lessons can be learned and applied in future scenarios.

upvoted 2 times

In a sample metric template, what does “target” mean?

- A. The suggested volume of data to collect
- B. The percentage of completion
- C. The threshold for a satisfactory rating
- D. The frequency at which the data is sampled

**Suggested Answer:** C

Community vote distribution

C (100%)

🗳️ 👤 **carlosbui** 7 months, 2 weeks ago

Should be C

upvoted 1 times

🗳️ 👤 **Ssourav** 10 months ago

**Selected Answer: C**

C. The threshold for a satisfactory rating

This means it's the desired or planned level of performance or achievement that the organization aims to reach for that specific metric.

upvoted 1 times

🗳️ 👤 **emily0922** 11 months ago

Should be C, with reference to NIST framework this is the defintion

upvoted 2 times

🗳️ 👤 **Alex951** 1 year, 1 month ago

**Selected Answer: C**

should be C

upvoted 2 times

🗳️ 👤 **mgmferreira** 1 year, 1 month ago

**Selected Answer: C**

No contexto de um modelo de métrica de amostra, "alvo" geralmente se refere ao limite ou ao objetivo que se deseja alcançar para considerar o resultado satisfatório. Por exemplo, se a métrica é a porcentagem de incidentes de privacidade resolvidos dentro de um determinado prazo, o "alvo" poderia ser 95%. Isso significa que a organização está visando resolver 95% dos incidentes de privacidade dentro desse prazo específico. Se o desempenho real atender ou exceder esse alvo, a organização pode considerá-lo satisfatório.

upvoted 2 times



Under which circumstances would people who work in human resources be considered a secondary audience for privacy metrics?

- A. They do not receive training on privacy issues
- B. They do not interface with the financial office
- C. They do not have privacy policy as their main task
- D. They do not have frequent interactions with the public

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **Ssourav** 10 months ago

**Selected Answer:** C

C. They do not have privacy policy as their main task

A secondary audience is typically those who are not directly involved in the main task or objective but still need the information for their respective roles. In this case, HR professionals might not have privacy policy as their main responsibility, but they still need to be aware of privacy metrics due to their involvement in other related tasks, such as employee training, onboarding, or internal policy enforcement.

upvoted 4 times

## SCENARIO -

Please use the following to answer the next question:

As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

You are charged with making sure that privacy safeguards are in place for new products and initiatives. What is the best way to do this?

- A. Hold a meeting with stakeholders to create an interdepartmental protocol for new initiatives
- B. Institute Privacy by Design principles and practices across the organization
- C. Develop a plan for introducing privacy protections into the product development stage
- D. Conduct a gap analysis after deployment of new products, then mend any gaps that are revealed

**Suggested Answer: B**

Community vote distribution

B (100%)

  **krishccie** 1 year ago

**Selected Answer: B**



privacy by design

upvoted 1 times

  **carlosbui** 1 year, 1 month ago

Should be B

upvoted 1 times

  **ET1857** 1 year, 2 months ago

**Selected Answer: B**

PbD covers the requirements phase also.

But C - starts with development phase

upvoted 2 times

  **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

B. Institute Privacy by Design principles and practices across the organization.

Privacy by Design principles ensure that privacy considerations are integrated from the very beginning and throughout the entire product or initiative development process. This proactive approach not only ensures that privacy safeguards are in place from the start but can also be more cost-effective in the long run as it helps prevent potential breaches or issues that might arise later, saving on potential fines, reputational damage, and corrective actions.

upvoted 3 times

  **emily0922** 1 year, 5 months ago

Should be B, B covers C also  
upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

The CEO likes what he's seen of the company's improved privacy program, but wants additional assurance that it is fully compliant with industry standards and reflects emerging best practices. What would best help accomplish this goal?

- A. An external audit conducted by a panel of industry experts
- B. An internal audit team accountable to upper management
- C. Creation of a self-certification framework based on company policies
- D. Revision of the strategic plan to provide a system of technical controls

**Suggested Answer: A**

*Community vote distribution*

A (100%)

 **Ssourav** Highly Voted 1 year, 4 months ago

**Selected Answer: A**

A. An external audit conducted by a panel of industry experts

This approach provides an independent, unbiased review of the company's privacy program. External experts can assess the company's processes and controls against industry standards, benchmarks, and emerging best practices. This will not only provide the desired assurance but also potentially enhance the company's credibility in the eyes of stakeholders, as it shows a willingness to be transparent and undergo external scrutiny.

upvoted 5 times

 **Vishwaji** Most Recent 1 year ago

**Selected Answer: A**

SHould be A

upvoted 1 times

 **carlosbui** 1 year, 1 month ago

should be A

upvoted 1 times

 **emily0922** 1 year, 4 months ago

I suggest A

upvoted 2 times

## SCENARIO -

Please use the following to answer the next question:

As the company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

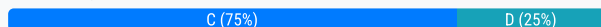
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

The company has achieved a level of privacy protection that established new best practices for the industry. What is a logical next step to help ensure a high level of protection?

- A. Brainstorm methods for developing an enhanced privacy framework
- B. Develop a strong marketing strategy to communicate the company's privacy practices
- C. Focus on improving the incident response plan in preparation for any breaks in protection
- D. Shift attention to privacy for emerging technologies as the company begins to use them

**Suggested Answer: C**

*Community vote distribution*



**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: C**

I agree with C and here's why. This is the most logical next step. Even with the best practices in place, no system is entirely immune from breaches. Improving the incident response plan ensures that the company can respond quickly and effectively to any potential privacy incidents, which is crucial for maintaining its reputation and protecting sensitive data.

For answer D, while this is important for long-term planning, the immediate next step should be to solidify existing privacy protections and have a well-prepared response plan. As the company starts to use emerging technologies, it's critical to have a strong foundation in place.

upvoted 2 times

**carlosbui** 7 months, 2 weeks ago

should be B

upvoted 1 times

**ET1857** 8 months, 1 week ago

**Selected Answer: C**

Improving on incident response plan should be the focus rather shifting the focus on new technologies because the program is mature enough to do due diligence before onboarding any new product for privacy impacts.

upvoted 3 times

**Cock** 8 months, 3 weeks ago

**Selected Answer: C**

By focusing on improving the incident response plan, the company can better prepare and respond in the event of any breaks in protection. This includes having a well-defined and tested plan in place, ensuring clear roles and responsibilities, establishing communication channels, and conducting regular drills and simulations to enhance the organization's ability to detect, respond to, and recover from any privacy incidents.

upvoted 4 times



  **Ssourav** 10 months ago

**Selected Answer: D**

D. Shift attention to privacy for emerging technologies as the company begins to use them.

Emerging technologies can introduce new and unforeseen privacy challenges. By proactively addressing privacy concerns in these areas, the company will be ahead of potential issues and continue to be an industry leader in privacy protection. It ensures that as the company adopts new technologies, they maintain their high standard of privacy protection.

upvoted 3 times

  **9385ae2** 5 months, 3 weeks ago

I think what sinks answer D are the words "shift attention". You don't want to stop focusing on core privacy controls. I think C is the best answer.

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

What metric can Goddard use to assess whether costs associated with implementing new privacy protections are justified?

- A. Compliance ratio
- B. Cost-effective mean
- C. Return on investment
- D. Implementation measure

**Suggested Answer: C**

Community vote distribution

C (100%)

 **Cock** 8 months, 3 weeks ago

**Selected Answer: C**

By calculating and analyzing the return on investment, Goddard can determine whether the costs associated with implementing new privacy protections are justified based on the expected financial benefits and potential long-term value to the company. This assessment helps him strike a balance between achieving the highest standards of privacy and being a responsible steward of the company's finances.

upvoted 1 times

 **Ssourav** 10 months ago

**Selected Answer: C**

C. Return on investment (ROI)

ROI is a common metric used to evaluate the profitability of an investment or to compare the profitability of several different investments. In the context of privacy protections, it would help determine the financial benefits received from the investment in privacy protections versus the costs associated with implementing them.

upvoted 1 times

## SCENARIO -

Please use the following to answer the next question:

As the company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that "appropriate" data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.

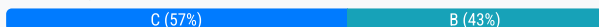
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. "We want Medialite to have absolutely the highest standards," he says. "In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective." You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.

You give a presentation to your CEO about privacy program maturity. What does it mean to have a "managed" privacy program, according to the AICPA/CICA Privacy Maturity Model?

- A. Procedures or processes exist, however they are not fully documented and do not cover all relevant aspects.
- B. Procedures and processes are fully documented and implemented, and cover all relevant aspects.
- C. Reviews are conducted to assess the effectiveness of the controls in place.
- D. Regular review and feedback are used to ensure continuous improvement toward optimization of the given process.

**Suggested Answer: C**

*Community vote distribution*



**Vinz\_** 6 months, 1 week ago

**Selected Answer: C**

C is the correct answer, as defined in the AICPA PMM  
upvoted 1 times

**Privacy2024** 6 months, 2 weeks ago

**Selected Answer: C**

Privacy Maturity Model PMM - is a well-established model that sets out maturity levels for privacy programs and operations. Adhoc, repeatable, defined, managed, optimized.

1. Adhoc - procedures or processes are generally informal, incomplete, and inconsistent.
  2. Repeatable - has procedures and processes but they are not fully documented, implemented, and cover all relevant aspects.
  3. Defined - processes are fully documented, implemented, and cover all relevant aspects.
  4. Managed - indicates that reviews are conducted to assess the effectiveness of the controls in place.
  5. Optimized - regular review and feedback are used to ensure continual improvement toward optimization of a given process. Each level builds on the previous one.
- upvoted 1 times

**MaritzTee** 7 months, 1 week ago

**Selected Answer: C**

B is for "defined." Managed is where you then have reviews conducted to evaluate the effectiveness of these controls to ensure they are meeting the organization's privacy objectives. This level of maturity involves ongoing monitoring and assessment to maintain and improve the privacy program over time.  
upvoted 2 times



🗨️ 👤 **MaritzTee** 7 months, 1 week ago

**Selected Answer: B**

B. Procedures and processes are fully documented and implemented, and cover all relevant aspects.

According to the AICPA/CICA Privacy Maturity Model, a "managed" privacy program means that procedures and processes are fully documented and implemented, and cover all relevant aspects. This indicates that the organization has established a comprehensive and systematic approach to privacy management, ensuring that all necessary elements are addressed and maintained effectively.

upvoted 2 times

🗨️ 👤 **thecheaterz** 7 months, 3 weeks ago

**Selected Answer: C**

From CIPM book - "Managed," or maturity level four, indicates that reviews are conducted to assess the effectiveness of the controls in place.

upvoted 2 times

🗨️ 👤 **DPRamone** 10 months ago

**Selected Answer: C**

C. Ref. <https://www.privacyauditorblog.com/2022/05/privacy-program-assessment-aicpa.html>

upvoted 2 times

🗨️ 👤 **carlosbui** 1 year, 1 month ago

should be B

upvoted 1 times

🗨️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: B**

B. Procedures and processes are fully documented and implemented, and cover all relevant aspects.

This is what it means to have a "managed" privacy program. The maturity levels typically progress from initial (ad hoc) to repeatable, defined, managed, and finally optimized. In the "managed" stage, processes are standardized, documented, and followed organization-wide.

upvoted 4 times

🗨️ 👤 **emily0922** 1 year, 4 months ago

C is correct, this is an accurate description of 'Managed'. For reference, the other options are:

A- Repeatable

B-Defined

D- Optimised

upvoted 3 times

Which of the following best demonstrates the effectiveness of a firm's privacy incident response process?

- A. The decrease of security breaches
- B. The decrease of notifiable breaches
- C. The increase of privacy incidents reported by users
- D. The decrease of mean time to resolve privacy incidents

**Suggested Answer:** D

Community vote distribution

D (80%)

C (20%)

🗳️ 👤 **DPRamone** 10 months ago

**Selected Answer: D**

Incident REPORT statistics say nothing about RESPONSE effectiveness. Hence D.  
upvoted 1 times

🗳️ 👤 **krishccie** 12 months ago

**Selected Answer: C**

<https://iapp.org/news/a/how-to-evaluate-your-privacy-incident-response-program/>  
upvoted 1 times

🗳️ 👤 **DPRamone** 10 months ago

Incident REPORT statistics say nothing about RESPONSE effectiveness. Hence D.  
upvoted 1 times

🗳️ 👤 **carlosbui** 1 year, 1 month ago

should be D  
upvoted 1 times

🗳️ 👤 **Ssourav** 1 year, 4 months ago

**Selected Answer: D**

D. The decrease of mean time to resolve privacy incidents

This best demonstrates the effectiveness of a firm's privacy incident response process. A decrease in the mean time to resolve privacy incidents indicates that the firm is becoming more efficient and effective at handling and resolving privacy-related issues when they arise.

upvoted 3 times