ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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.

Answer: C

Question: 2

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.

Answer: C

Question: 3

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.

Answer: D

Question: 4

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.

Answer: C

Question: 5

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Eurek a. 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.

Answer: B

Question: 6

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Eurek a. 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.

Answer: C

Question: 7

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Eurek a. 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.

Answer: D

Question: 8

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Eurek a. 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.

Answer: B

Question: 9

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.

Answer: C

Question: 10

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.

Answer: A

Question: 11

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat
a. 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.

Answer: D

Question: 12

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat
a. 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.

Answer: C

Question: 13

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat
a. 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.

Answer: A

Question: 14

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat
a. 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.

Answer: A

Question: 15

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat

a. 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.

Answer: D

Question: 16

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.

Answer: C

Question: 17

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.

Answer: A

Question: 18

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.

Answer: C

Question: 19

As a Data Protection Officer, 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.

Answer: D

Question: 20

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 21

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: B

Question: 22

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 23

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 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.

Answer: B

Question: 24

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.

Answer: C

Question: 25

SCENARIO
Please use the following to answer the next QUESTIO N:

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 done in order to modernize the office, mostly in regard to the handling of clients' personal dat a. 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.

Answer: A

Question: 26

SCENARIO
Please use the following to answer the next QUESTIO N:

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 done in order to modernize the office, mostly in regard to the handling of clients' personal dat a. 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.

Answer: C

Question: 27

SCENARIO
Please use the following to answer the next QUESTIO N:

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 done in order to modernize the office, mostly in regard to the handling of clients' personal dat a. 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.

Answer: B

Question: 28

SCENARIO
Please use the following to answer the next QUESTIO N:

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 done in order to modernize the office, mostly in regard to the handling of clients' personal dat a. 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.

Answer: D

Question: 29

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.

Answer: B

Question: 30

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 onviolators.
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.

Answer: C

Question: 31

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.

Answer: B

Question: 32

SCENARIO

Please use the following to answer the next QUESTIO N:

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 dat
a. 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.

Answer: C

Question: 33

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat
a. 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).

Answer: A

Question: 34

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat
a. 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.

Answer: A

Question: 35

SCENARIO
Please use the following to answer the next QUESTIO N:

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 dat

a. 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.

Answer: B

Question: 36

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.
C. The Human Resources Director.
D. The organization's General Counsel.

Answer: A

Question: 37

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.

Answer: B

Question: 38

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.

Answer: B

Question: 39

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: D

Question: 40

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Consolidated'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.

Answer: A

Question: 41

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Consolidated's current privacy program?

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

Answer: D

Question: 42

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 43

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 44

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Consolidated?

A. Privacy by Design.
B. Privacy Step Assessment.
C. Information Security Planning.
D. Innovation Privacy Standards.

Answer: A

Question: 45

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.

Answer: B

Question: 46

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.

Answer: C

Question: 47

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

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

Answer: D

Question: 48

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.

Answer: A

Question: 49

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.

Answer: A

Question: 50

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.

Answer: D

Question: 51

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.

Answer: D

Question: 52

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 53

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 54

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: B

Question: 55

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 56

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.

Answer: A

Question: 57

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.

Answer: D

Question: 58

SCENARIO
Please use the following to answer the next QUESTIO N:

Natalia, 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, 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 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.

Answer: B

Question: 59

SCENARIO

Please use the following to answer the next QUESTIO N:

Natalia, 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, 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 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.

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.

Answer: A

Question: 60

SCENARIO
Please use the following to answer the next QUESTIO N:

Natalia, 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, 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 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.

Answer: B

Question: 61

SCENARIO

Please use the following to answer the next QUESTIO N:

Natalia, 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, 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 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.

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.

Answer: A

Question: 62

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.

Answer: C

Question: 63

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.

Answer: C

Question: 64

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.

Answer: A

Question: 65

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.

Answer: A

Question: 66

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.

Answer: D

Question: 67

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: B

Question: 68

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 69

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: D

Question: 70

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.

Answer: C

Question: 71

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.

Answer: D

Question: 72

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: B

Question: 73

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 74

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 75

SCENARIO
Please use the following to answer the next QUESTIO N:

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 vetting.

Answer: D

Question: 76

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: B

Question: 77

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.

Answer: C

Question: 78

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.

Answer: B

Question: 79

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.

Answer: D

Question: 80

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.

Answer: D

Question: 81

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 82

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 83

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.

Answer: C

Question: 84

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 85

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

Answer: C

Question: 86

SCENARIO

Please use the following to answer the next QUESTIO N:

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.

Answer: A

Question: 87

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.

Answer: A

Question: 88

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.

Answer: B

Question: 89

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.

Answer: D

Question: 90

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.

Answer: D

Question: 91

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

Answer: C

Question: 92

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Accountans)/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 dat a. 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 in 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)

Answer: D

Question: 93

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Accountans)/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 dat a. 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 in 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

Answer: B

Question: 94

SCENARIO

Please use the following to answer the next QUESTIO N:

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 Accountans)/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 dat a. 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 in 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

Answer: B

Question: 95

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Accountans)/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 dat a. 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 in 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

Answer: B

Question: 96

SCENARIO

Please use the following to answer the next QUESTIO N:

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 Accountans)/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 dat

a. 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 in 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

Answer: B

Question: 97

SCENARIO
Please use the following to answer the next QUESTIO N:

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

Answer: B

Question: 98

SCENARIO
Please use the following to answer the next QUESTIO N:

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 Accountans)/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 dat a. 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 in 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

Answer: B

Question: 99

"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

Answer: C

Question: 100

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

Answer: B

Question: 101

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

Answer: D

Question: 102

SCENARIO
Please use the following to answer the next QUESTIO N:

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."

Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. 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 providers 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.

Answer: B

Question: 103

SCENARIO
Please use the following to answer the next QUESTIO N:

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."

Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. 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

Answer: C

Question: 104

SCENARIO
Please use the following to answer the next QUESTIO N:

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."

Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. 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

Answer: A

Question: 105

SCENARIO

Please use the following to answer the next QUESTIO N:

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."

Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. 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

Answer: A

Question: 106

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

Answer: B

Question: 107

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

Answer: D

Question: 108

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.

Answer: C

Question: 109

SCENARIO
Please use the following to answer the next QUESTIO N:

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:

1. Send an enrollment invitation to everyone the day after the contract is signed.
2. Enroll someone with just their first name and the last-4 of their national identifier.
3. Monitor each enrollee's credit for two years from the date of enrollment.
4. Send a monthly email with their credit rating and offers for credit-related services at market rates.

5. 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

Answer: D

Question: 110

SCENARIO
Please use the following to answer the next QUESTIO N:

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:

1. Send an enrollment invitation to everyone the day after the contract is signed.
2. Enroll someone with just their first name and the last-4 of their national identifier.
3. Monitor each enrollee's credit for two years from the date of enrollment.
4. Send a monthly email with their credit rating and offers for credit-related services at market rates. 5. 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.

Answer: B

Question: 111

SCENARIO
Please use the following to answer the next QUESTIO N:

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:

1. Send an enrollment invitation to everyone the day after the contract is signed.
2. Enroll someone with just their first name and the last-4 of their national identifier.
3. Monitor each enrollee's credit for two years from the date of enrollment.
4. Send a monthly email with their credit rating and offers for credit-related services at market rates.
5. 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

Answer: C

Question: 112

SCENARIO
Please use the following to answer the next QUESTIO N:

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:

1. Send an enrollment invitation to everyone the day after the contract is signed.
2. Enroll someone with just their first name and the last-4 of their national identifier.

3. Monitor each enrollee's credit for two years from the date of enrollment.
4. Send a monthly email with their credit rating and offers for credit-related services at market rates. 5. 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

Answer: C

Question: 113

SCENARIO
Please use the following to answer the next QUESTIO N:

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:

1. Send an enrollment invitation to everyone the day after the contract is signed.
2. Enroll someone with just their first name and the last-4 of their national identifier.
3. Monitor each enrollee's credit for two years from the date of enrollment.
4. Send a monthly email with their credit rating and offers for credit-related services at market rates. 5. 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

Answer: C

Question: 114

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

Answer: C

Question: 115

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

Answer: C

Question: 116

SCENARIO
Please use the following to answer the next QUESTIO N:

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

Answer: B

Question: 117

SCENARIO
Please use the following to answer the next QUESTIO N:

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

Answer: A

Question: 118

SCENARIO
Please use the following to answer the next QUESTIO N:

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 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

Answer: D

Question: 119

SCENARIO
Please use the following to answer the next QUESTIO N:

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

Answer: C

Question: 120

SCENARIO
Please use the following to answer the next QUESTIO N:

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 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.

Answer: B

Question: 121

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

Answer: D

Question: 122

Which of the following is TRUE about a PIA (Privacy Impact Analysis)?

A. Any project that involves the use of personal data requires a PIA
B. A Data Protection Impact Analysis (DPIA) process includes a PIA
C. The PIA must be conducted at the early stages of the project lifecycle
D. The results from a previous information audit can be leveraged in a PIA process

Answer: D

Question: 123

SCENARIO
Please use the following to answer the next QUESTIO N:

Martin Briseño is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseño decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseño to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseño's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality

Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseño and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They

planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

In the Information Technology engineers had originally set the default for customer credit card information to "Do Not Save," this action would have been in line with what concept?

A. Use limitation
B. Privacy by Design
C. Harm minimization
D. Reactive risk management

Answer: B

Question: 124

SCENARIO
Please use the following to answer the next QUESTIO N:

Martin Briseño is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseño decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseño to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseño's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseño and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

What key mistake set the company up to be vulnerable to a security breach?

A. Collecting too much information and keeping it for too long
B. Overlooking the need to organize and categorize data
C. Failing to outsource training and data management to professionals
D. Neglecting to make a backup copy of archived electronic files

Answer: B

Question: 125

SCENARIO

Please use the following to answer the next QUESTIO N:

Martin Briseño is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseño decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseño to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseño's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and

unused. Briseño and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

How would a strong data life cycle management policy have helped prevent the breach?

A. Information would have been ranked according to importance and stored in separate locations
B. The most sensitive information would have been immediately erased and destroyed
C. The most important information would have been regularly assessed and tested for security D. Information would have been categorized and assigned a deadline for destruction

Answer: D

Question: 126

SCENARIO
Please use the following to answer the next QUESTIO N:

Martin Briseño is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseño decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseño to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseño's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who

completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseño and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

How was Pacific Suites responsible for protecting the sensitive information of its offshoot, PHT?

A. As the parent company, it should have transferred personnel to oversee the secure handling of PHT's data.

B. As the parent company, it should have performed an assessment of PHT's infrastructure and confirmed complete separation of the two networks.

C. As the parent company, it should have ensured its existing data access and storage procedures were integrated into PHT's system.

D. As the parent company, it should have replaced PHT's electronic files with hard-copy documents stored securely on site.

Answer: C

Question: 127

SCENARIO
Please use the following to answer the next QUESTIO N:

Martin Briseño is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseño decided to change the hotel's on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseño to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseño's program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user's name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT's profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e-learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program's systems and records remained in Pacific Suites' digital archives, un-accessed and unused. Briseño and Silva-Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific

Hospitality Training's customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity.

What must Pacific Suite's primary focus be as it manages this security breach?

A. Minimizing the amount of harm to the affected individuals
B. Investigating the cause and assigning responsibility
C. Determining whether the affected individuals should be notified
D. Maintaining operations and preventing publicity

Answer: A

Question: 128

A Human Resources director at a company reported that a laptop containing employee payroll data was lost on the train. Which action should the company take IMMEDIATELY?

A. Report the theft to law enforcement
B. Wipe the hard drive remotely
C. Report the theft to the senior management
D. Perform a multi-factor risk analysis

Answer: D

Question: 129

Read the following steps:
Perform frequent data back-ups.
Perform test restorations to verify integrity of backed-up data.
Maintain backed-up data ofline or on separate servers.

These steps can help an organization recover from what?

A. Phishing attacks
B. Authorization errors
C. Ransomware attacks
D. Stolen encryption keys

Answer: C

Question: 130

The General Data Protection Regulation (GDPR) specifies fines that may be levied against data controllers for certain infringements. Which of the following will be subject to administrative fines of up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year?

A. Failure to demonstrate that consent was given by the data subject to the processing of their personal data where it is used as the basis for processing
B. Failure to implement technical and organizational measures to ensure data protection is enshrined by design and default
C. Failure to process personal information in a manner compatible with its original purpose
D. Failure to provide the means for a data subject to rectify inaccuracies in personal data

Answer: B

Question: 131

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 security controls are missing from the Eureka program?

A. Storage of medical data in the cloud is not permissible under the General Data Protection Regulation (GDPR)
B. Data access is not limited to those who "need to know" for their role
C. Collection of data without a defined purpose might violate the fairness principle
D. Encryption of the data at rest prevents European users from having the right of access and the right of portability of their data

Answer: B

Question: 132

What is the main purpose in notifying data subjects of a data breach?

A. To avoid financial penalties and legal liability
B. To enable regulators to understand trends and developments that may shape the law
C. To ensure organizations have accountability for the sufficiency of their security measures
D. To allow i ndividuals to take any actions required to protect the mselves from possible consequences

Answer: D

Question: 133

Under the General Data Protection Regulation (GDPR), which situation would be LEAST likely to require a Data Protection Impact Assessment (DPIA)?

A. A health clinic processing its patients' genetic and health data
B. The use of a camera system to monitor driving behavior on highways
C. A Human Resources department using a tool to monitor its employees' internet activity
D. An online magazine using a mailing list to send a generic daily digest to marketing emails

Answer: D

Question: 134

Under the General Data Protection Regulation (GDPR), which of the following situations would LEAST likely require a controller to notify a data subject?

A. An encrypted USB key with sensitive personal data is stolen
B. A direct marketing email is sent with recipients visible in the 'cc' field
C. Personal data of a group of individuals is erroneously sent to the wrong mailing list
D. A hacker publishes usernames, phone numbers and purchase history online after a cyber-attack

Answer: A

Question: 135

SCENARIO

Please use the following to answer the next QUESTIO N:

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 establish the current baseline of Ace Space's privacy maturity, Penny should consider all of the following factors EXCEPT?

A. Ace Space's documented procedures
B. Ace Space's employee training program
C. Ace Space's vendor engagement protocols
D. Ace Space's content sharing practices on social media

Answer: D

Question: 136

SCENARIO
Please use the following to answer the next QUESTIO N:

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.

What is the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has?

A. Analyze the data inventory to map data flows
B. Audit all vendors' privacy practices and safeguards
C. Conduct a Privacy Impact Assessment for the company
D. Review all cloud contracts to identify the location of data servers used

Answer: A

Question: 137

SCENARIO
Please use the following to answer the next QUESTIO N:
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.

What information will be LEAST crucial from a privacy perspective in Penny's review of vendor contracts?

A. Audit rights
B. Liability for a data breach
C. Pricing for data security protections
D. The data a vendor will have access to

Answer: C

Question: 138

Which of the documents below assists the Privacy Manager in identifying and responding to a request from an individual about what personal information the organization holds about then with whom the information is shared?

A. Risk register
B. Privacy policy
C. Records retention schedule
D. Personal information inventory

Answer: D

Question: 139

Which of the following is the optimum first step to take when creating a Privacy Officer governance model?

A. Involve senior leadership.
B. Provide flexibility to the General Counsel Office.
C. Develop internal partnerships with IT and information security.
D. Leverage communications and collaboration with public affairs teams.

Answer: A

Question: 140

Which of the following helps build trust with customers and stakeholders?

A. Only publish what is legally necessary to reduce your liability.
B. Enable customers to view and change their own personal information within a dedicated portal.
C. Publish your privacy policy using broad language to ensure all of your organization's activities are captured.
D. Provide a dedicated privacy space with the privacy policy, explanatory documents and operation frameworks.

Answer: D

Question: 141

Which of the following is NOT an important factor to consider when developing a data retention policy?

A. Technology resource.
B. Business requirement.
C. Organizational culture.
D. Compliance requirement

Answer: C

Question: 142

When supporting the business and data privacy program expanding into a new jurisdiction, it is important to do all of the following EXCEPT?

A. Identify the stakeholders.
B. Appoint a new Privacy Officer (PO) for that jurisdiction.
C. Perform an assessment of the laws applicable in that new jurisdiction.
D. Consider culture and whether the privacy framework will need to account for changes in culture.

Answer: B

Question: 143

When building a data privacy program, what is a good starting point to understand the scope of privacy program needs?

A. Perform Data Protection Impact Assessments (DPIAs).
B. Perform Risk Assessments
C. Complete a Data Inventory.
D. Review Audits.

Answer: C

Question: 144

Which of the following actions is NOT required during a data privacy diligence process for Merger & Acquisition (M&A) deals?

A. Revise inventory of applications that house personal data and data mapping.
B. Update business processes to handle Data Subject Requests (DSRs).
C. Compare the original use of personal data to post-merger use.
D. Perform a privacy readiness assessment before the deal.

Answer: D

Question: 145

When devising effective employee policies to address a particular issue, which of the following should be included in the first draft?

A. Rationale for the policy.
B. Points of contact for the employee.
C. Roles and responsibilities of the different groups of individuals.
D. Explanation of how the policy is applied within the organization.

Answer: A

Question: 146

Your company wants to convert paper records that contain customer personal information into electronic form, upload the records into a new third-party marketing tool and then merge the customer personal information in the marketing tool with information from other applications. As the Privacy Officer, which of the following should you complete to effectively make these changes?

A. A Record of Authority.
B. A Personal Data Inventory.
C. A Privacy Threshold Analysis (PTA).
D. A Privacy Impact Assessment (PIA).

Answer: D

Question: 147

A minimum requirement for carrying out a Data Protection Impact Assessment (DPIA) would include?

A. Processing on a large scale of special categories of data.
B. Monitoring of a publicly accessible area on a large scale.
C. Assessment of the necessity and proportionality.
D. Assessment of security measures.

Answer: A

Question: 148

Which of the following best supports implementing controls to bring privacy policies into effect?

A. The internal audit department establishing the audit controls which test for policy effectiveness.

B. The legal department or outside counsel conducting a thorough review of the privacy program and policies.

C. The Chief Information Officer as part of the Senior Management Team creating enterprise privacy policies to ensure controls are available.

D. The information technology (IT) group supporting and enhancing the privacy program and privacy policy by developing processes and controls.

Answer: D

Question: 149

What is most critical when outsourcing data destruction service?

A. Obtain a certificate of data destruction.
B. Confirm data destruction must be done on-site.
C. Conduct an annual in-person audit of the provider's facilities.
D. Ensure that they keep an asset inventory of the original data.

Answer: A

Question: 150

Data retention and destruction policies should meet all of the following requirements EXCEPT?

A. Data destruction triggers and methods should be documented.

B. Personal information should be retained only for as long as necessary to perform its stated purpose.

C. Documentation related to audit controls (third-party or internal) should be saved in a nonpermanent format by default.

D. The organization should be documenting and reviewing policies of its other functions to ensure alignment (e.g. HR, business development, finance, etc.).

Answer: C

Question: 151

What is least likely to be achieved by implementing a Data Lifecycle Management (DLM) program?

A. Reducing storage costs.
B. Ensuring data is kept for no longer than necessary.
C. Crafting policies which ensure minimal data is collected.
D. Increasing awareness of the importance of confidentiality.

Answer: C

Question: 152

There are different forms of monitoring available for organizations to consider when aligning with their privacy program goals.
Which of the following forms of monitoring is best described as 'auditing'?

A. Evaluating operations, systems, and processes.
B. Tracking, reporting and documenting complaints from all sources.
C. Assisting in the completion of attesting reporting for SOC2, ISO, or BS7799.
D. Ensuring third parties have appropriate security and privacy requirements in place.

Answer: A

Question: 153

Which will best assist you in quickly identifying weaknesses in your network and storage?

A. Running vulnerability scanning tools.
B. Reviewing your privacy program metrics.
C. Reviewing your role-based access controls.
D. Establishing a complaint-monitoring process.

Answer: A

Question: 154

Which of the following is NOT a type of privacy program metric?

A. Business enablement metrics.
B. Data enhancement metrics.
C. Value creation metrics.
D. Risk-reduction metrics.

Answer: B

Question: 155

How do privacy audits differ from privacy assessments?

A. They are non-binding.
B. They are evidence-based.
C. They are based on standards.
D. They are conducted by external parties.

Answer: B

Question: 156

An organization's internal audit team should do all of the following EXCEPT?

A. Implement processes to correct audit failures.
B. Verify that technical measures are in place.
C. Review how operations work in practice.
D. Ensure policies are being adhered to.

Answer: A

Question: 157

"Respond" in the privacy operational lifecycle includes which of the following?

A. Information security practices and functional area integration.
B. Privacy awareness training and compliance monitoring.
C. Communication to stakeholders and alignment to laws.

D. Information requests and privacy rights requests.

Answer: D

Question: 158

If your organization has a recurring issue with colleagues not reporting personal data breaches, all of the following are advisable to do EXCEPT?

A. Carry out a root cause analysis on each breach to understand why the incident happened.
B. Communicate to everyone that breaches must be reported and how they should be reported.
C. Provide role-specific training to areas where breaches are happening so they are more aware.
D. Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.

Answer: D

Question: 159

Which of the following information must be provided by the data controller when complying with GDPR "right to be informed" requirements?

A. The purpose of personal data processing.
B. The data subject's right to withdraw consent
C. The contact details of the Data Protection Officer (DPO).
D. The name of any organizations with whom personal data was shared.

Answer: C

Question: 160

If done correctly, how can a Data Protection Impact Assessment (DPIA) create a win/win scenario for organizations and individuals?

A. By quickly identifying potentially problematic data attributes and reducing the risk exposure.
B. By allowing Data Controllers to solicit feedback from individuals about how they feel about the potential data processing.
C. By enabling Data Controllers to be proactive in their analysis of processing activities and ensuring compliance with the law.
D. By better informing about the risks associated with the processing activity and improving the

organization's transparency with individuals.

Answer: D

Question: 161

Which of the following is NOT recommended for effective Identity Access Management?

A. Demographics.
B. Unique user IDs.
C. User responsibility.
D. Credentials (e.g.. password).

Answer: A

Question: 162

You would like to better understand how your organization can demonstrate compliance with international privacy standards and identify gaps for remediation. What steps could you take to achieve this objective?

A. Carry out a second-party audit.
B. Consult your local privacy regulator.
C. Conduct an annual self assessment.
D. Engage a third-party to conduct an audit.

Answer: D

Question: 163

If your organization has a recurring issue with colleagues not reporting personal data breaches, all of the following are advisable to do EXCEPT?

A. Review reporting activity on breaches to understand when incidents are being reported and when they are not to improve communication and training.
B. Improve communication to reinforce to everyone that breaches must be reported and how they should be reported.
C. Provide role-specific training to areas where breaches are happening so they are more aware.
D. Distribute a phishing exercise to all employees to test their ability to recognize a threat attempt.

Answer: D

Question: 164

A systems audit uncovered a shared drive folder containing sensitive employee data with no access controls and therefore was available for all employees to view. What is the first step to mitigate further risks?

A. Notify all employees whose information was contained in the file.
B. Check access logs to see who accessed the folder.
C. Notify legal counsel of a privacy incident.
D. Restrict access to the folder.

Answer: D

Question: 165

While trying to e-mail her manager, an employee has e-mailed a list of all the company's customers, including their bank details, to an employee with the same name at a different company. Which of the following would be the first stage in the incident response plan under the General Data Protection Regulation (GDPR)?

A. Notification to data subjects.
B. Containment of impact of breach.
C. Remediation offers to data subjects.
D. Notification to the Information Commissioner's Office (ICO).

Answer: B

Question: 166

Which of the following is NOT a type of privacy program metric?
A. Business enablement metrics.
B. Data enhancement metrics.
C. Value creation metrics.
D. Commercial metrics.

Answer: C

Question: 167

Your company provides a SaaS tool for B2B services and does not interact with individual consumers. A client's current employee reaches out with a right to delete request. what is the most appropriate response?

A. Forward the request to the contact on file for the client asking them how they would like you to proceed.

B. Redirect the individual back to their employer to understand their rights and how this might impact access to company tools.

C. Process the request assuming that the individual understands the implications to their organization if their information is deleted.

D. Explain you are unable to process the request because business contact information and associated data is not covered under privacy rights laws.

Answer: B

Question: 168

When a data breach incident has occurred. the first priority is to determine?

A. Who caused the breach.
B. How the breach occurred.
C. How to contain the breach.
D. When the breach occurred.

Answer: C

Question: 169

Which of the following is NOT a main technical data control area?

A. Obfuscation.
B. Tokenization.
C. Access controls.
D. Data minimization.

Answer: A

Question: 170

Integrating privacy requirements into functional areas across the organization happens at which stage of the privacy operational life cycle?

A. Assessing data.
B. Protecting personal data.
C. Sustaining program performance.
D. Responding to requests and incidents.

Answer: C

Question: 171

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.

Answer: D

Question: 172

Under the GDPR. when the applicable lawful basis for the processing of personal data is a legal obligation with which the controller must comply. which right can the data subject exercise?

A. Right to withdraw consent.
B. Right to data portability.
C. Right to restriction.
D. Right to erasure.

Answer: C

Question: 173

Which of the following is a physical control that can limit privacy risk?

A. Keypad or biometric access.
B. user access reviews.
C. Encryption.
D. Tokenization.

Answer: A

Question: 174

Under the General Data Protection Regulation (GDPR), what are the obligations of a processor that engages a sub-processor?

A. The processor must give the controller prior written notice and perform a preliminary audit of the sub-processor.
B. The processor must Obtain the controllers specifiC written authorization and provide annual reports on the sub-processor'S performance.
C. The processor must receive a written agreement that the sub-processor will be fully liable to the controller for the performance of its obligations in relation to the personal data concerned.
D. The processor must obtain the consent of the controller and ensure the sub-processor complies with data processing obligations that are equivalent to those that apply to the processor.

Answer: D

Question: 175

When conducting due diligence during an acquisition, what should a privacy professional avoid?

A. Discussing with the acquired company the type and scope of their data processing.
B. Allowing legal in both companies to handle the privacy laws and compliance.
C. Planning for impacts on the data processing operations post-acquisition.
D. Benchmarking the two Companies privacy policies against one another.

Answer: B

Question: 176

An online retailer detects an incident involving customer shopping history but no keys have been compromised. The Privacy Offce is most concerned when it also involves?

A. Internal unique personal identifiers.
B. Plain text personal identifiers.
C. Hashed mobile identifiers.
D. No personal identifiers.

Answer: B

Question: 177

Your marketing team wants to know why they need a check box for their SMS opt-in. You explain it is part of the consumer's right to?

A. Request correction.
B. Raise complaints.
C. Have access.
D. Be informed.

Answer: D

Question: 178

SCENARIO
Please use the following to answer the next question
You were recently hired by InStyte Date Corp as a privacy manager to help InStyle Data Corp become compliant with a new data protection law
The law mandates that businesses have reasonable and appropriate security measures in place to protect personal dat
a. Violations of that mandate are heavily fined and the legislators have stated that they will aggressively pursue companies that don t comply with the new law
You are paved with a security manager and tasked with reviewing InStyle Data Corp s current state and advising the business how it can meet the "reasonable and appropriate security" requirement InStyle Data Corp has grown rapidly and has not kept a data inventory or completed a data mapping InStyte Data Corp has also developed security-related policies ad hoc and many have never been implemented The various teams involved in the creation and testing of InStyle Data Corp s products experience significant turnover and do not

have well defined roles There's little documentation addressing what personal data is processed by which product and for what purpose

Work needs to begin on this project immediately so that InStyle Data Corp can become compliant by the time the law goes into effect. You and you partner discover that InStyle Data Corp regularly sends files containing sensitive personal data back to its customers through email sometimes using InStyle Data Corp employees personal email accounts. You also team that InStyle Data Corp s privacy and information security teams are not informed of new personal data flows, new products developed by InStyte Data Corp that process personal data, or updates to existing InStyle Data Corp products that may change what or how the personal data is processed until after the product or update has gone have.

Through a review of InStyle Date Corp's test and development environment logs, you discover InStyle Data Corp sometimes gives login credentials to any InStyle Data Corp employee or contractor who requests them. The test environment only contains dummy data but the development environment contains personal data including Social Security Numbers, hearth ^formation and financial information All credentialed InStyle Data Corp employees and contractors have the ability to after and delete personal data in both environments regardless of their role or what project they are working on.

You and your partner provide a gap assessment citing the issues you spotted, along with recommended remedial actions and a method to measure implementation InStyle Data Corp implements all of the recommended security controls You review the processes roles, controls and measures taken to appropriately protect the personal data at every stop However, you realize there is no plan for monitoring and nothing in place addressing sanctions for violations of the updated policies and procedures InStyle Data Corp pushes back, stating they do not have the resources for such monitoring.

What aspect of the data management life cycle will still be unaddressed it you cannot find the resources to become compliant?

A. Auditability.
B. Enforcement
C. Irretrievability
D. Access management

Answer: B

Question: 179

SCENARIO

Please use the following to answer the next question

You were recently hired by InStyte Date Corp as a privacy manager to help InStyle Data Corp become compliant with a new data protection law

The law mandates that businesses have reasonable and appropriate security measures in place to protect personal dat

a. Violations of that mandate are heavily fined and the legislators have stated that they will aggressively pursue companies that don t comply with the new law

You are paved with a security manager and tasked with reviewing InStyle Data Corp s current state and advising the business how it can meet the "reasonable and appropriate security" requirement InStyle Data Corp has grown rapidly and has not kept a data inventory or completed a data mapping InStyte Data Corp has also developed security-related policies ad hoc and many have never been implemented The various teams involved in the creation and testing of InStyle Data Corp s products experience significant turnover and do not have well defined roles There's little documentation addressing what personal data is processed by which product and for what purpose

Work needs to begin on this project immediately so that InStyle Data Corp can become compliant by the time the law goes into effect. You and you partner discover that InStyle Data Corp regularly sends files containing sensitive personal data back to its customers through email sometimes using InStyle Data Corp employees personal email accounts. You also team that InStyle Data Corp s privacy and information security teams are not informed of new personal data flows, new products developed by InStyte Data Corp that process personal data, or updates to existing InStyle Data Corp products that may change what or how the personal data is processed until after the product or update has gone have.

Through a review of InStyle Date Corp's test and development environment logs, you discover InStyle Data Corp sometimes gives login credentials to any InStyle Data Corp employee or contractor who requests them. The test environment only contains dummy data but the development environment contains personal data including Social Security Numbers, hearth ^formation and financial information All credentialed InStyle Data Corp employees and contractors have the ability to after and delete personal data in both environments regardless of their role or what project they are working on.

You and your partner provide a gap assessment citing the issues you spotted, along with recommended remedial actions and a method to measure implementation InStyle Data Corp implements all of the recommended security controls You review the processes roles, controls and measures taken to appropriately protect the personal data at every stop However, you realize there is no plan for monitoring and nothing in place addressing sanctions for violations of the updated policies and procedures InStyle Data Corp pushes back, stating they do not have the resources for such monitoring.

Having completed the gap assessment, you and your partner need to first undertake a thorough review of?

A. Data life cyde
B. Security policies.
C. System development life cycle.
D. Privacy Impact (PIA).

Answer: C

Question: 180

All of the following should be mandatory in the contract for the outsourced vendor EXCEPT?

A. Generation of reports and metrics.
B. Information security controls.
C. Liability for data breach.
D. Cyber insurance.

Answer: D

Question: 181

All of the following would address your concern of the copy room EXCEPT?

A. Placing a paper shredder in the copy room.

B. Initiating a PIA.
C. Hanging a poster reminding users to shred paper.
D. Implementing a new paper record destruction policy.

Answer: B

Question: 182

Which most accurately describes the reasons an organization will conduct a PIA?

A. To assess an organization's compliance with applicable laws, regulations, standards, and internal procedures.
B. To establish an inventory of its data processing activities in compliance with Article 30 of the GDPR.
C. To identify and reduce the privacy risks to individuals at the commencement of a project.
D. To analyze the impact of an incident response and determine next steps.

Answer: C

Question: 183

All of the following would be recommended for effective identity access management (IAM) EXCEPT?

A. User responsibility.
B. Demographics.
C. Biometrics.
D. Credentials.

Answer: B

Question: 184

What is the main purpose in notifying data subjects of a data breach?

A. To avoid financial penalties and legal liability.
B. To enable regulators to understand trends and developments that may shape the law.
C. To ensure organizations have accountability for the sufficiency of their security measures.
D. To allow individuals to take any actions required to protect themselves from possible consequences.

Answer: D

Question: 185

With whom would it be best for a privacy professional in an organization to consult regarding Privacy-Enhancing Technologies (PETs)?

A. A specialist focused on AI.
B. An independent privacy technology advocate.
C. An engineer who designs information security technology products.
D. An information technologist specializing in information privacy technology.

Answer: D

Question: 186

Which of the following is the most likely way an independent privacy organization might work to promote sound privacy practices?

A. By developing principles for self-regulation.
B. By enacting new legislation.
C. By completing on-site audits.
D. By issuing penalties for violations of rules.

Answer: A

Question: 187

In a mobile app for purchasing and selling concert tickets, users are prompted to create a personalized profile prior to engaging in transactions. Once registered, users can securely access their profiles within the app, empowering them to manage and modify personal data as needed. Which foundational Privacy by Design (PbD) principle does this feature follow?

A. Proactive, not reactive; preventative, not remedial.
B. Full functionality — positive-sum, not zero-sum.
C. Respect for user privacy - keep it user-centric.
D. End-to-end security — full life cycle protection.

Answer: C

Question: 188

All of the following would be answered through the creation of a data inventory EXCEPT?

A. Where the data is located.
B. How the data is protected.
C. How the data is being used.
D. What the format of the data is.

Answer: D

Question: 189

All of the following are access control measures required by the Payment Card Industry Data Security Standard (PCI DSS) EXCEPT?

A. Restrict physical access to cardholder data.
B. Update antivirus software before granting access.
C. Assign a unique ID to each person with computer access.
D. Restrict access to cardholder data by business need-to-know.

Answer: B

Question: 190

A privacy maturity model provides all of the following EXCEPT?

A. A standard reference to assess a privacy program's current level of development.
B. A way to highlight what functions a company lacks for proper program management.
C. A way to guarantee that a company is compliant with applicable laws and regulations.
D. An example of the methods and practices necessary to evaluate a company's level of risk.

Answer: C

Question: 191

The main reason the response to this incident should be integrated into the Business Continuity Plan (BCP) is because?

A. The repercussions for the company could have significant environmental impacts.
B. The need for retraining employees will be paramount.
C. Major stakeholders are involved from every critical area of the business.
D. The impact on the company's competitive advantage is potentially significant.

Answer: C

Question: 192

The theft of proprietary information could have best been prevented by?

A. Doing criminal background checks on all contractors.
B. Having requests for access reviewed by the privacy office.
C. Escalating access requests for approval by the appropriate data custodian.
D. Requiring multi-factor authentication for contractor access to confidential company data.

Answer: D

Question: 193

According to the General Data Protection Regulation (GDPR), the requirements of a Data Protection Impact Assessment (DPIA) include that it?

A. Be reported to the corresponding supervisory authority.
B. Publish the report to demonstrate the transparency of the data processing.
C. Provide a description of the proposed processing operation and its purpose.
D. Is required if the processing activity entails risk to the rights and freedoms of an EU individual.

Answer: C

Question: 194

A start-up tech company is developing its privacy policies and processes.
Which policy is most important to ensure the organization is successful at processing consumer health information?

A. The employee notice.
B. The consumer health data policy.
C. The privacy impact assessment (PIA).
D. The Health Insurance Portability and Accountability Act (HIPAA) privacy notice.

Answer: B

Question: 195

The first step an organization should take when considering the use of a third-party's AI-based resume ranking tool is to?

A. Secure stakeholder buy-in and approval to ensure the tool meets the organization's requirements. B. Conduct an assessment of the tool's impact both on privacy and on conformity with applicable AI regulation.

C. Distribute a notice to the candidates whose resumes the tool will assess to ensure they understand and consent to the use of the tool.

D. Secure appropriate contractual concessions to ensure that the developer is primarily responsible for any violation of applicable privacy law.

Answer: B

Question: 196

SCENARIO

Please use the following to answer the next QUESTIO N:

Liam is the newly appointed information technology (IT) compliance manager at Mesa, a USbased outdoor clothing brand with a global E-commerce presence. During his second week, he is contacted by the company's IT audit manager, who informs him that the auditing team will be conducting a review of Mesa's privacy compliance risk in a month.

A bit nervous about the audit, Liam asks his boss what his predecessor had completed related to privacy compliance before leaving the company. Liam is told that a consent management tool had been added to the website and they commissioned a privacy risk evaluation from a small consulting firm last year that determined that their risk exposure was relatively low given their current control environment. After reading the consultant's report, Liam realized that the scope of the assessment was limited to breach notification laws in the US and the Payment Card Industry's Data Security Standard (PCI DSS).

Not wanting to let down his new team, Liam kept his concerns about the report to himself and figured he could try to put some additional controls into place before the audit. Having some privacy compliance experience in his last role, Liam thought he might start by having discussions with the Ecommerce and marketing teams.

The E-commerce Director informed him that they were still using the cookie consent tool forcibly placed on the home screen by the CIO, but could not understand the point since their office was not located in California or Europe. The marketing director touted his department's success with purchasing email lists and taking a shotgun approach to direct marketing. Both directors highlighted their tracking tools on the website to enhance customer experience while learning more about where else the customer had shopped. The more people Liam met with, the more it became apparent that privacy awareness and the general control environment at Mesa needed help. With three weeks before the audit, Liam updated Mesa's Privacy Notice himself, which was taken and revised from a competitor's website. He also wrote policies and procedures outlining the roles and responsibilities for privacy within Mesa and distributed the document to all departments he knew of with access to personal information.

During this time. Liam also filled the backlog of data subject requests for deletion that had been sent to him by the customer service manager. Liam worked with application owners to remove these individual's information and order history from the customer relationship management (CRM) tool, the enterprise resource planning (ERP). the data warehouse and the email server.

At the audit kick-off meeting. Liam explained to his boss and her team that there may still be some room for improvement, but he thought the risk had been mitigated to an appropriate level based on the work he had done thus far.

After the audit had been completed, the audit manager and Liam met to discuss her team's findings, and much to his dismay. Liam was told that none of the work he had completed prior to the audit followed best practices for governance and risk mitigation. In fact, his actions only opened the company up to additional risk and scrutiny. Based on these findings. Liam worked with external counsel and an established privacy consultant to develop a remediation plan.

Given the feedback provided to Liam after the audit, what maturity level would the audit team most likely have assigned to Mesa's privacy policies and procedures if they use the Privacy Maturity Model (PMM)?

A. Repeatable.
B. Ad-hoc.
C. Defined.
D. Managed.

Answer: B

Question: 197

An organization can use Privacy-Enhancing Technologies (PETs) to?

A. Replace current technical controls.
B. Strengthen existing privacy controls.
C. Ensure compliance with local privacy regulations.
D. Produce data for the privacy professional to interpret.

Answer: B

Question: 198

All of the following are accurate regarding the use of technical security controls EXCEPT?

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.

Answer: C

Question: 199

What is the main reason for conducting a data inventory or data map of your organization?

A. To test the security of your organization's main data systems.
B. To assess different methods for collecting data by your organization.
C. To know where your organization’s data is located and how it is used.
D. To evaluate whether your vendors have the required policies and procedures in place.

Answer: C

Question: 200

A new business crafting its privacy policy is struggling with how it will define the term "personal data." Which of the following should inform this decision?

A. The types of special categories of data being processed.
B. The business's requirements for storing collected data.
C. The amount of data the business expects to collect.
D. The privacy laws to which the business is subject.

Answer: D

Question: 201

When developing a privacy program and selecting a program sponsor or "champion" the least important consideration should be that they?

A. Are a part of the organization's top management
B. Have the authority to approve policy and provide funding.
C. Will be an effective advocate and understand the importance of privacy.
D. Have accountability for the organization's privacy and/or information security, risk, compliance or legal decisions.

Answer: A

Question: 202

K a privacy professional wants to show that an organization's privacy program is working as intended, the professional should?

A. Collect feedback from customers about the privacy program.
B. Carry out a personal data breach tabletop exercise.
C. Collect and analyze privacy program metrics.
D. Review privacy policies.

Answer: A

Question: 203

Training and awareness metrics in a privacy program are necessary to?

A. Identify data breaches.
B. Implement privacy policies.
C. Demonstrate compliance with regulations.
D. Educate customers on the organization's data practices.

Answer: C

Question: 204

Which of the following would be least beneficial in integrating privacy requirements and representation into functional areas across an organization?

A. Creating a structure that provides a communication chain (formally and informally) that a privacy professional can use in performing key data protection activities.
B. Creating a governance structure composed of representatives from each business function and geographic region in which the organization has a presence.
C. Creating a program where the privacy officer (or privacy team) can lead on privacy matters by having exclusive responsibility to execute the privacy mission.
D. Creating a privacy committee or council composed of various stakeholders.

Answer: C

Question: 205

When implementing an organization's privacy program, what right should be granted to the data subject?

A. To have their data amended or erased if errors are found.
B. To limit or refuse the disclosure of their data for any reason.
C. To provide feedback regarding an organization's privacy policy.
D. To verify that an organization uses the highest level of privacy protection available.

Answer: A

Question: 206

Under the General Data Protection Regulation (GDPR), international data transfer is allowed using the mechanisms in all of the following scenarios EXCEPT between companies who?

A. Are part of the same group of enterprise using approved Binding Corporate Rules (BCRs).
B. Have signed up to the EU Standard Contractual Clauses.
C. Have put in place a binding confidentiality agreement.
D. Have put in place an approved code of conduct.

Answer: C

Question: 207

SCENARIO
Please use the following to answer the next QUESTIO N:
Liam is the newly appointed information technology (IT) compliance manager at Mesa, a USbased outdoor clothing brand with a global E-commerce presence. During his second week, he is contacted by the company's IT audit manager, who informs him that the auditing team will be conducting a review of Mesa's privacy compliance risk in a month.
A bit nervous about the audit, Liam asks his boss what his predecessor had completed related to privacy compliance before leaving the company. Liam is told that a consent management tool had been added to the website and they commissioned a privacy risk evaluation from a small consulting firm last year that determined that their risk exposure was relatively low given their current control environment. After reading the consultant's report, Liam realized that the scope of the assessment was limited to breach notification laws in the US and the Payment Card Industry's Data Security Standard (PCI DSS).
Not wanting to let down his new team, Liam kept his concerns about the report to himself and figured he could try to put some additional controls into place before the audit. Having some privacy compliance experience in his last role, Liam thought he might start by having discussions with the Ecommerce and marketing teams.

The E-commerce Director informed him that they were still using the cookie consent tool forcibly placed on the home screen by the CIO, but could not understand the point since their office was not located in California or Europe. The marketing director touted his department's success with purchasing email lists and taking a shotgun approach to direct marketing. Both directors highlighted their tracking tools on the website to enhance customer experience while learning more about where else the customer had shopped. The more people Liam met with, the more it became apparent that privacy awareness and the general control environment at Mesa needed help. With three weeks before the audit, Liam updated Mesa's Privacy Notice himself, which was taken and revised from a competitor's website. He also wrote policies and procedures outlining the roles and responsibilities for privacy within Mesa and distributed the document to all departments he knew of with access to personal information.

During this time. Liam also filled the backlog of data subject requests for deletion that had been sent

to him by the customer service manager. Liam worked with application owners to remove these individual's information and order history from the customer relationship management (CRM) tool, the enterprise resource planning (ERP). the data warehouse and the email server.

At the audit kick-off meeting. Liam explained to his boss and her team that there may still be some room for improvement, but he thought the risk had been mitigated to an appropriate level based on the work he had done thus far.

After the audit had been completed, the audit manager and Liam met to discuss her team's findings, and much to his dismay. Liam was told that none of the work he had completed prior to the audit followed best practices for governance and risk mitigation. In fact, his actions only opened the company up to additional risk and scrutiny. Based on these findings. Liam worked with external counsel and an established privacy consultant to develop a remediation plan.

Why do Mesa's E-commerce and marketing efforts need to be compliant with the GDPR?

A. Mesa is US-based.
B. Mesa uses mailing lists and engages in direct marketing.
C. Mesa uses automated systems and tools to process personal data.
D. Mesa has a global E-commerce presence and may have customers in Europe.

Answer: D

Question: 208

SCENARIO

Please use the following to answer the next QUESTIO N:

Liam is the newly appointed information technology (IT) compliance manager at Mesa, a USbased outdoor clothing brand with a global E-commerce presence. During his second week, he is contacted by the company's IT audit manager, who informs him that the auditing team will be conducting a review of Mesa's privacy compliance risk in a month.

A bit nervous about the audit, Liam asks his boss what his predecessor had completed related to privacy compliance before leaving the company. Liam is told that a consent management tool had been added to the website and they commissioned a privacy risk evaluation from a small consulting firm last year that determined that their risk exposure was relatively low given their current control environment. After reading the consultant's report, Liam realized that the scope of the assessment was limited to breach notification laws in the US and the Payment Card Industry's Data Security Standard (PCI DSS).

Not wanting to let down his new team, Liam kept his concerns about the report to himself and figured he could try to put some additional controls into place before the audit. Having some privacy compliance experience in his last role, Liam thought he might start by having discussions with the Ecommerce and marketing teams.

The E-commerce Director informed him that they were still using the cookie consent tool forcibly placed on the home screen by the CIO, but could not understand the point since their office was not located in California or Europe. The marketing director touted his department's success with purchasing email lists and taking a shotgun approach to direct marketing. Both directors highlighted their tracking tools on the website to enhance customer experience while learning more about where else the customer had shopped. The more people Liam met with, the more it became apparent that privacy awareness and the general control environment at Mesa needed help.

With three weeks before the audit, Liam updated Mesa's Privacy Notice himself, which was taken and revised from a competitor's website. He also wrote policies and procedures outlining the roles and responsibilities for privacy within Mesa and distributed the document to all departments he knew of with access to personal information.

During this time. Liam also filled the backlog of data subject requests for deletion that had been sent to him by the customer service manager. Liam worked with application owners to remove these individual's information and order history from the customer relationship management (CRM) tool, the enterprise resource planning (ERP). the data warehouse and the email server.

At the audit kick-off meeting. Liam explained to his boss and her team that there may still be some room for improvement, but he thought the risk had been mitigated to an appropriate level based on the work he had done thus far.

After the audit had been completed, the audit manager and Liam met to discuss her team's findings, and much to his dismay. Liam was told that none of the work he had completed prior to the audit followed best practices for governance and risk mitigation. In fact, his actions only opened the company up to additional risk and scrutiny. Based on these findings. Liam worked with external counsel and an established privacy consultant to develop a remediation plan.

All of the key phases of an audit have occurred with Liam's involvement in the situation EXCEPT?

A. Prepare.
B. Audit.
C. Report.
D. Follow-up.

Answer: A

Question: 209

SCENARIO

Please use the following to answer the next QUESTIO N:

Liam is the newly appointed information technology (IT) compliance manager at Mesa, a USbased outdoor clothing brand with a global E-commerce presence. During his second week, he is contacted by the company's IT audit manager, who informs him that the auditing team will be conducting a review of Mesa's privacy compliance risk in a month.

A bit nervous about the audit, Liam asks his boss what his predecessor had completed related to privacy compliance before leaving the company. Liam is told that a consent management tool had been added to the

website and they commissioned a privacy risk evaluation from a small consulting firm last year that determined that their risk exposure was relatively low given their current control environment. After reading the consultant's report, Liam realized that the scope of the assessment was limited to breach notification laws in the US and the Payment Card Industry's Data Security Standard (PCI DSS).

Not wanting to let down his new team, Liam kept his concerns about the report to himself and figured he could try to put some additional controls into place before the audit. Having some privacy compliance experience in his last role, Liam thought he might start by having discussions with the Ecommerce and marketing teams.

The E-commerce Director informed him that they were still using the cookie consent tool forcibly placed on the home screen by the CIO, but could not understand the point since their office was not located in California or Europe. The marketing director touted his department's success with purchasing email lists and taking a shotgun approach to direct marketing. Both directors highlighted their tracking tools on the website to enhance customer experience while learning more about where else the customer had shopped.

The more people Liam met with, the more it became apparent that privacy awareness and the general control environment at Mesa needed help. With three weeks before the audit, Liam updated Mesa's Privacy Notice himself, which was taken and revised from a competitor's website. He also wrote policies and procedures outlining the roles and responsibilities for privacy within Mesa and distributed the document to all departments he knew of with access to personal information.

During this time. Liam also filled the backlog of data subject requests for deletion that had been sent to him by the customer service manager. Liam worked with application owners to remove these individual's information and order history from the customer relationship management (CRM) tool, the enterprise resource planning (ERP). the data warehouse and the email server.

At the audit kick-off meeting. Liam explained to his boss and her team that there may still be some room for improvement, but he thought the risk had been mitigated to an appropriate level based on the work he had done thus far.

After the audit had been completed, the audit manager and Liam met to discuss her team's findings, and much to his dismay. Liam was told that none of the work he had completed prior to the audit followed best practices for governance and risk mitigation. In fact, his actions only opened the company up to additional risk and scrutiny. Based on these findings. Liam worked with external counsel and an established privacy consultant to develop a remediation plan.

What key error related to program governance did Liam make prior to the audit kick-off meeting?

A. He did not properly escalate his concerns and develop a remediation plan with leadership support.
B. He met with stakeholders in marketing and E-commerce without the auditors.
C. He did not conduct a data inventory assessment prior to adopting the policy.
D. He asked stakeholders to delete customer data out of the CRM tool.

Answer: A

Question: 210

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

A. Managing the data flows from parties outside the region.
B. Establishing legal requirements for privacy protection in the region.
C. Promoting privacy protection technologies developed in the region.

D. Promoting consumer trust and business confidence in cross-border data flows.

Answer: D

Question: 211

What steps can an organization take to ensure its data inventory is kept up to date?

A. Identify a process owner for each processing activity in the data inventory.
B. Conduct an annual review of the data inventory against the Privacy Notice.
C. Review the data inventory when there are changes to laws and regulations.
D. Link the data inventory to the implementation of new systems or applications.

Answer: B

Question: 212

The purpose of a data flow map is to help an organization do all of the following EXCEPT?

A. Determine unidentified opportunities for information collection.
B. Assist compliance with privacy-related laws and regulations.
C. Identify any.
D. Recognize who in the organization has access to what information.

Answer: A

Question: 213

What is the key privacy objective in undertaking an evaluation of technical controls?

A. To review and evaluate gaps in targeted internal privacy awareness training.
B. To determine if the current privacy framework is adequate for the company's needs.
C. To evaluate and mitigate third-party risk associated with service provider relationships.
D. To identify and mitigate privacy risks associated with technical systems and data processing activities.

Answer: D

Question: 214

Which risk-analysis exercise required by GDPR balances the benefits of a specific processing operation involving personal data against the potential for harm to data subjects?

A. Privacy Impact Assessment (PIA).
B. Transfer Impact Assessment (TIA).
C. Data Protection Impact Assessment (DPIA).
D. Legitimate Interest Impact Assessment (LIIA).

Answer: A

Question: 215

When vetting third-party processors of data protected by the GDPR. why is it important to know the physical location of stored personal data from clients?

A. To determine their incidence response time.
B. To determine the country laws that would govern the contract.
C. To determine the likelihood of a security breach in the location.
D. To ensure the country has adequate protection or if safeguards are required.

Answer: D

Question: 216

Which item below best represents how a privacy group can effectively communicate with functional areas?

A. Work independently and share the knowledge with functional groups.
B. Work closely with functional areas by acting as both an advisor and an advocate.
C. Choose a work unit representative and funnel all communications through that one person.
D. Monitor the responsibilities of managers who are responsible for the privacy of functional areas.

Answer: B

Question: 217

A company's human resources (HR) group is working with their information security team lo tag data within their systems as ''special data" or "sensitive data" What is the most probable reason for the group to do so?

A. To ensure the data is fully controlled and used for only authorized purposes.
B. To apply the organization's data deletion standard.
C. To create a robust record of processing activities.
D. To prepare for an upcoming regulatory audit under GDPR.

Answer: D

Question: 218

Which of the following is a common disadvantage of a third-party audit?

A. It identifies weaknesses of internal controls.
B. It lends credibility to an internal audit program.
C. It requires a learning curve about the organization.
D. It provides a level of unbiased, expert recommendations.

Answer: C

Question: 219

A "right to erasure" request could be rejected if the processing of personal data is for?

A. An outdated original purpose.
B. Compliance with legal obligation.
C. The offer of information society services.
D. The establishment of personal legal claims.

Answer: B

Question: 220

Post-liquidation, a company that has acquired assets would require separate consent from a data subject if personally identifiable data were being retained for which purpose?

A. For tax purposes.
B. For analytical purposes.
C. To be able to ensure payment of pension funds.
D. To secure employment benefits for former employees.

Answer: B

Question: 221

During a merger and acquisition, the most comprehensive review of privacy risks and gaps occurs when conducting what activity?

A. Transfer Impact Assessment (TIA).
B. Risk identification review.
C. Due diligence.
D. Integration.

Answer: C

Question: 222

Your company's lead applied scientist believes there's an opportunity to proactively address customer issues using machine learning. She requests access to all of the company's customer data and several publicly available datasets
All the following are appropriate next steps EXCEPT?

A. Understanding the geographic location of your customers.
B. Providing a public disclosure to all customers describing the purpose and nature of processing.
C. Checking your company's public privacy notice to ensure this processing Is in line with current disclosures.
D. Requesting further Information from your scientist to understand the goal of the model and the eventual operational description.

Answer: A

Question: 223

All of the following are components of a data collection notice EXCEPT?

A. The categories of information shared with third parties
B. The length of time the personal information will be stored.
C. The meta-data which could be generated from collection of the information.
D. The lawful interests pursued by the responsible party collecting the information.

Answer: C

Question: 224

Privacy/security questionnaires are used primarily to do what?

A. Map data flows.
B. Assess vendor risk.
C. Determine access controls.
D. Comply with contractual requirements.

Answer: B

Question: 225

SCENARIO

Please use the following lo answer the next QUESTIO N:

You are the privacy manager within the privacy office of a National Forest Parks and Recreation Department. While having lunch with a colleague from the IT division, you learn that the IT director has put out a request for proposal (RFP) which calls for a system that collects the personal data of park attendees.

You consult with a few other colleagues in IT and learn that the RFP is worded such that it leaves it to the vendors to demonstrate what information they would collect from people who enter parks anywhere in the country, either in a vehicle or on foot. A partial list of the information collected includes:

- personal identifiers such as name, address, age, gender;
- vehicle registration information:
- facial images of park attendees;
- health information (e.g.. physical disabilities, use of mobility devices)

The stated purpose of the RFP is to:

"Improve the National Forest. Parks, and Recreation Department's ability to track and monitor service usage thereby Increasing the robustness of our customer data and to improve service offerings."

Companies have already started submitting proposals for software solutions that address these information gathering practices. There is only one week left before the RFP closes.

The IT department has put together an RFP evaluation team but no one from the privacy office has been a Dart of the RFP ud to this point. This occurred deposite the fact….

All of the following are appropriate for the privacy office in developing a privacy assessment metric EXCEPT?

A. Clarifying what data fields are to be collected, including use cases for all purposes.
B. Canceling this RFP and re-issuing it after thorough consultation with your office.
C. Obtaining a list of vendors and the services they are offering in response to the RFP requirements. D. Extending the deadline for the RFP giving your office more time to assess the privacy needs of the program.

Answer: A

Question: 226

SCENARIO

Please use the following lo answer the next QUESTIO N:

You are the privacy manager within the privacy office of a National Forest Parks and Recreation Department. While having lunch with a colleague from the IT division, you learn that the IT director has put out a request for proposal (RFP) which calls for a system that collects the personal data of park attendees.

You consult with a few other colleagues in IT and learn that the RFP is worded such that it leaves it to the vendors to demonstrate what information they would collect from people who enter parks anywhere in the country, either in a vehicle or on foot. A partial list of the information collected includes:

- personal identifiers such as name, address, age, gender;
- vehicle registration information:
- facial images of park attendees;
- health information (e.g.. physical disabilities, use of mobility devices)

The stated purpose of the RFP is to:
"Improve the National Forest. Parks, and Recreation Department's ability to track and monitor service usage thereby Increasing the robustness of our customer data and to improve service offerings."
Companies have already started submitting proposals for software solutions that address these information gathering practices. There is only one week left before the RFP closes.
The IT department has put together an RFP evaluation team but no one from the privacy office has been a Dart of the RFP ud to this point. This occurred deposite the fact….
Which of the following data protection actions has been implemented by the National Forest Parks and Recreation Department?

A. Policy creation.
B. Data minimization.
C. Sufficient engagement with the privacy team.
D. Identification of all of the sources, types and uses of personal information(PI).

Answer: D

Question: 227

SCENARIO
Please use the following lo answer the next QUESTIO N:
You are the privacy manager within the privacy office of a National Forest Parks and Recreation Department. While having lunch with a colleague from the IT division, you learn that the IT director has put out a request for proposal (RFP) which calls for a system that collects the personal data of park attendees.
You consult with a few other colleagues in IT and learn that the RFP is worded such that it leaves it to the vendors to demonstrate what information they would collect from people who enter parks anywhere in the country, either in a vehicle or on foot. A partial list of the information collected includes:

- personal identifiers such as name, address, age, gender;
- vehicle registration information:
- facial images of park attendees;
- health information (e.g.. physical disabilities, use of mobility devices)

The stated purpose of the RFP is to:
"Improve the National Forest. Parks, and Recreation Department's ability to track and monitor service usage thereby Increasing the robustness of our customer data and to improve service offerings."
Companies have already started submitting proposals for software solutions that address these information gathering practices. There is only one week left before the RFP closes.
The IT department has put together an RFP evaluation team but no one from the privacy office has been a Dart of the RFP ud to this point. This occurred deposite the fact….
From a privacy management perspective, what is problematic about the "stated purpose" of the RFP?

A. It seeks to improve the robustness of customer data.
B. It seeks to track and monitor service usage by the customers.
C. It could lead to unauthorized collection of personal data to improve customer service.
D. It does not specify what information will be collected for improving customer data.

Answer: D

Question: 228

SCENARIO

Please use the following lo answer the next QUESTIO N:

You are the privacy manager within the privacy office of a National Forest Parks and Recreation Department. While having lunch with a colleague from the IT division, you learn that the IT director has put out a request for proposal (RFP) which calls for a system that collects the personal data of park attendees.

You consult with a few other colleagues in IT and learn that the RFP is worded such that it leaves it to the vendors to demonstrate what information they would collect from people who enter parks anywhere in the country, either in a vehicle or on foot. A partial list of the information collected includes:

- personal identifiers such as name, address, age, gender;
- vehicle registration information:
- facial images of park attendees;
- health information (e.g.. physical disabilities, use of mobility devices)

The stated purpose of the RFP is to:

"Improve the National Forest. Parks, and Recreation Department's ability to track and monitor service usage thereby Increasing the robustness of our customer data and to improve service offerings."

Companies have already started submitting proposals for software solutions that address these information gathering practices. There is only one week left before the RFP closes.

The IT department has put together an RFP evaluation team but no one from the privacy office has been a Dart of the RFP ud to this point. This occurred deposite the fact….

Which of the following is the least important privacy consideration associated with assessing data when implementing a large-scale project like this?

A. Standardization of privacy safeguards on a national scale.
B. Classification of the types of personal information collected by the system
C. Identifying operational risks associated with data storage, access and disposal.
D. Third-party vendor assessment to determine how well privacy practices of vendors align with your organization's practices.

Answer: B

Question: 229

Under the GDPR, what obligation does a data controller or processor have after appointing a data protection officer (DPO)?

A. To submit for approval to the DPO a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.
B. To provide resources necessary to carry out the defined tasks of the DPO and to maintain their expert knowledge.

C. To ensure that the DPO acts as the sole point of contact for individuals' questions about their personal data.

D. To ensure that the DPO receives sufficient instructions regarding the exercise of their defined tasks.

Answer: B

Question: 230

Creating a privacy governance model for an organization that is required to appoint data protection officers under the GDPR poses what additional challenge?

A. They must react without delay to suppliers.
B. They must reply personally to data subjects.
C. They must report directly to top management.
D. They must respond immediately to employees.

Answer: C

Question: 231

Protection from threats to facilities, systems that process and store electronic copies and IT work/equipment locations best describes which category of security control?

A. Physical Control.
B. Technical Control.
C. Geographic Control.
D. Administrative Control.

Answer: A

Question: 232

Which of the following methods analyzes data collected based the scale and not the endpoint of the privacy program?

A. Trend Analysis.
B. Business Resiliency.
C. Return on Investment.
D. The Privacy Maturity Model.

Answer: D

Question: 233

A marketing team regularly exports spreadsheets to use (or analysis including customer name, birthdate and home address. These spreadsheets are routinely shared between members of various teams via email even with employees that do not need such granular data.

What is the best way to lower overall risk?

A. Set up security measures in the company's email client to prevent spreadsheets with customer information from accidentally being sent to external recipients.

B. Anonymize exportable data by creating categories of information, like age range and geographic region.

C. Allow the free exchange of information to continue but require spreadsheets be password protected.

D. Allow only certain users to export customer data from the database.

Answer: B

Question: 234

SCENARIO

Please use the following lo answer the next QUESTIO N:

The board risk committee of your organization is particularly concerned not only by the number and frequency of data breaches reported to it over the past 12 months, but also the inconsistency in responses and poor incident response turnaround times.

Upon reviewing the current incident response plan (IRP), it was discovered that while the business continuity plan (BCP> had been updated on time, the IRP, linked to BCP. was last updated over three years ago.

The board risk committee has noted this as high risk especially since company policy is to review and update policies and plans annually. Consequently, the newly appointed data protection officer (DPO) was requested to provide a paper on how she would remediate the situation.

As a seasoned data privacy professional, you have been requested to assist the new DPO.

Your first recommendation in addressing the board risk committee's concerns is to?

A. Integrate the IRP into the BCP so it is not a stand-alone document.

B. Conduct a table-top exercise based on the version of the IRP that is currently on record.

C. Focus on training and awareness sessions in order to familiarize relevant staff with current policies and procedures.

D. Update the IRP with the applicable emergency contact information, policies and procedures, as well as timelines and action steps.

Answer: D

Question: 235

SCENARIO
Please use the following lo answer the next QUESTIO N:
The board risk committee of your organization is particularly concerned not only by the number and frequency of data breaches reported to it over the past 12 months, but also the inconsistency in responses and poor incident response turnaround times.
Upon reviewing the current incident response plan (IRP), it was discovered that while the business continuity plan (BCP) had been updated on time, the IRP, linked to BCP. was last updated over three years ago.
The board risk committee has noted this as high risk especially since company policy is to review and update policies and plans annually. Consequently, the newly appointed data protection officer (DPO) was requested to provide a paper on how she would remediate the situation.
As a seasoned data privacy professional, you have been requested to assist the new DPO.
Which additional proactive step listed below would best mitigate these risks in the future?

A. Make the IRP a live document that is evaluated for completeness during each incident.
B. Make copies of the IRP in various place so it can be accessed remotely or when ofline.
C. Add comments about incidents to the IRP to record what action was taken.
D. Make sure that everyone listed in the IRP has a copy of the IRP

Answer: A

Question: 236

A Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) are conducted during what phase of a System Development Life Cycle (SDLC)?

A. Testing.
B. Design.
C. Deployment.
D. Maintenance.

Answer: B

Question: 237

Which of the following controls are generally NOT part of a PIA review?

A. Access.

B. Incident.
C. Retention.
D. Collection.

Answer: B

Question: 238

Under the European Data Protection Board (EDPB). which processing operation would require a DPIA?

A. An online newspaper using its subscriber list to email a daily newsletter.
B. A healthcare clinic that processes personal data of its patients in its billing system.
C. A hospital processing patient's genetic and health data in its hospital information system.
D. An online store displaying advertisements based on items viewed or purchased on its own website.

Answer: C

Question: 239

After an incident, all of the following are potential objectives for improvements to the way an organization handles breach management EXCEPT?

A. Contacting regulators.
B. Reviewing lessons learned.
C. Ensuring appropriate privacy/security funding.
D. Getting commitment from stakeholders related to any process updates.

Answer: A

Question: 240

You are the privacy officer at a university. Recently, the police have contacted you as they suspect that one of your students is using a library computer to commit financial fraud. The police would like your assistance in investigating this individual and are requesting computer logs and usage data of the student.
What Is your first step in responding to the request?

A. Refuse the request as the police do not have a warrant.
B. Provide the data to police and record it for your own archives.
C. Contact the university's legal counsel to determine if the request is lawful.
D. Review policies, procedures and legislation to determine the university's obligation to co-operate with the police.

Answer: C

Question: 241

PbD is the framework that?

A. Dictates the design of the system development life cycle.
B. Establishes risk-based expectations for privacy management.
C. Embeds privacy into the design of technology, systems and practices.
D. Guides organizations in designing, implementing and managing privacy programs in line with privacy laws and best practices.

Answer: C

Question: 242

Last year Ecosoft 8150 was hacked and a number of servers and programs were affected. Since the incident, the company started collecting metrics on data privacy and system outages to try to stop it from happening in the future.
What analysis would be most helpful based on the data they have collected?

A. Return on Investment (ROI).
B. Compliance analysis.
C. Business Resiliency.
D. Trend analysis.

Answer: D