Number: CIPM
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: CIPM
Exam Name: Certified Information Privacy Manager

Exam A

QUESTION 1
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear. Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
Based on the scenario, what additional change will increase the effectiveness of the privacy compliance hotline?

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

Correct Answer: B
Section:
Explanation:
Based on the scenario, an additional change that will increase the effectiveness of the privacy compliance hotline is a system for staff education. A privacy compliance hotline is a mechanism for employees, customers, or other stakeholders to report any concerns or violations of the company's privacy policy or applicable laws. However, a hotline alone is not sufficient to ensure a robust and compliant privacy program. Employees also need to be educated and trained on the importance of privacy, the company's privacy policy and procedures, their roles and responsibilities, and the consequences of non-compliance. A system for staff education can help raise awareness, foster a culture of privacy, and prevent or mitigate potential risks.Reference: [Privacy Compliance Hotline], [Staff Education]

QUESTION 2
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.

Correct Answer: A
Section:
Explanation:

If an organization maintains a separate ethics office, its officer would typically report to the Board of Directors in order to retain the greatest degree of independence.This is because the Board of Directors is the highest governing body of the organization and has the authority and responsibility to oversee the ethical conduct and performance of the organization and its management1Reporting to the Board of Directors would enable the ethics officer to avoid any potential conflicts of interest or undue influence from other senior executives or managers who may have a stake in the ethical issues or decisions that the ethics office handles2Reporting to the Board of Directors would also enhance the credibility and legitimacy of the ethics office and its recommendations, as well as demonstrate the organization's commitment to ethical values and culture3
The other options are not as suitable as reporting to the Board of Directors for retaining the greatest degree of independence for the ethics office.Reporting to the Chief Financial Officer may create a conflict of interest or a perception of bias if the ethical issues or decisions involve financial matters or implications4Reporting to the Human Resources Director may limit the scope or authority of the ethics office to deal with ethical issues or decisions that go beyond human resources policies or practices5Reporting to the organization's General Counsel may blur the distinction or create confusion between legal compliance and ethical conduct, as well as raise concerns about attorney-client privilege or confidentiality6Reference:1:Board Responsibilities | BoardSource;2:Ethics Officer: Job Description, Duties and Requirements;3:The Role Of The Ethics And Compliance Officer In The 21st Century | Corporate Compliance Insights;4:Ethics Officer: Job Description, Duties and Requirements;5:Ethics Officer: Job Description, Duties and Requirements;6:Ethics Officer: Job Description, Duties and Requirements

QUESTION 3
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.

Correct Answer: D
Section:
Explanation:
This is an example of Privacy by Design (PbD), which is an approach to systems engineering that integrates privacy into the design and development of products, services, and processes from the outset7PbD aims to ensure that privacy is embedded into the core functionality of any system or service, rather than being added as an afterthought or a trade-off.PbD is based on seven foundational principles: proactive not reactive; preventive not remedial; privacy as the default setting; privacy embedded into design; full functionality -- positive-sum, not zero-sum; end-to-end security -- full lifecycle protection; visibility and transparency -- keep it open; and respect for user privacy -- keep it user-centric8

QUESTION 4
Which is TRUE about the scope and authority of data protection oversight authorities?

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

Correct Answer: C
Section:
Explanation:
The true statement about the scope and authority of data protection oversight authorities is that no one agency officially oversees the enforcement of privacy regulations in the United States. Unlike other regions, such as the European Union or Canada, the United States does not have a comprehensive federal privacy law or a single national data protection authority. Instead, it has a patchwork of sector-specific and state-level laws and regulations, enforced by various federal and state agencies, such as the Federal Trade Commission (FTC), the Department of Health and Human Services (HHS), the Department of Commerce (DOC), etc. Additionally, individuals can also bring private lawsuits against organizations that violate their privacy rights.Reference: [Data Protection Authorities], [Privacy Law in the United States]

QUESTION 5
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.

Correct Answer: B
Section:
Explanation:
A privacy professional should keep in mind that the number of metrics should be limited at first when selecting which metrics to collect. Metrics are quantitative measures that help evaluate the performance and effectiveness of a privacy program. However, collecting too many metrics can be overwhelming, confusing, and costly. Therefore, a privacy professional should start with a few key metrics that are relevant, meaningful, actionable, and aligned with the organization's privacy goals and priorities. These metrics can be refined and expanded over time as the privacy program matures and evolves.Reference: [Privacy Metrics], [Measuring Privacy Program Effectiveness]

QUESTION 6
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear. Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
What Data Lifecycle Management (DLM) principle should the company follow if they end up allowing departments to interpret the privacy policy differently?

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

Correct Answer: C
Section:
Explanation:
If the company ends up allowing departments to interpret the privacy policy differently, they should follow the Data Lifecycle Management (DLM) principle of adequately documenting reasons for inconsistencies.This principle requires that data should be accurate, complete, and consistent throughout its lifecycle and that any deviations or discrepancies should be justified and recorded1This would help the company to maintain data quality and integrity, as well as to demonstrate accountability and compliance with data protection regulations2
The other options are not DLM principles that the company should follow if they allow departments to interpret the privacy policy differently.Proving the authenticity of the company's records is a principle related to data preservation and archiving, not data interpretation3Arranging for official credentials for staff members is a principle related to data access and security, not data interpretation4Creating categories to reflect degrees of data importance is a principle related to data classification and retention, not data interpretation5Reference:1:Data Lifecycle Management: A Complete Guide | Splunk;2:Data Lifecycle Management | IBM;3:Data Preservation | Digital Preservation Handbook;4:Data Access Management Best Practices | Smartsheet;5:Data Classification: What It Is And How To Do It | Varonis

QUESTION 7
SCENARIO
Please use the following to answer the next QUESTION:

Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.
With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear.
Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
What is the most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is NOT adequate?

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

Correct Answer: A
Section:
Explanation:
The most likely reason the Chief Information Officer (CIO) believes that generating a list of needed IT equipment is not adequate is that the company needs to have policies and procedures in place to guide the purchasing decisions.Policies and procedures are essential for ensuring that the IT equipment meets the business needs and objectives, as well as the legal and regulatory requirements for data protection and security6Policies and procedures can help the company to:
Define the roles and responsibilities of the IT staff and other stakeholders involved in the purchasing process.
Establish the criteria and standards for selecting and evaluating the IT equipment vendors and products.
Determine the budget and timeline for acquiring and deploying the IT equipment.
Implement the best practices for installing, configuring, testing, maintaining, and disposing of the IT equipment.
Monitor and measure the performance and effectiveness of the IT equipment.
Without policies and procedures in place, the company may face risks such as:
Wasting time and money on unnecessary or inappropriate IT equipment.
Exposing sensitive data to unauthorized access or loss due to inadequate or incompatible IT equipment.
Failing to comply with data protection laws or industry standards due to non-compliant or outdated IT equipment.
Facing legal or reputational consequences due to data breaches or incidents caused by faulty or insecure IT equipment.
Therefore, generating a list of needed IT equipment is not adequate without having policies and procedures in place to guide the purchasing decisions.Reference:6: IT Policies & Procedures: A Quick Guide - ProjectManager;7: IT Policies & Procedures: A Quick Guide - ProjectManager

QUESTION 8
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.

Correct Answer: C
Section:
Explanation:
Binding Corporate Rules (BCRs) are a mechanism for international organizations to transfer personal data within their group of companies across different jurisdictions, in compliance with the EU General Data Protection Regulation (GDPR) and other privacy laws. BCRs are legally binding and enforceable by data protection authorities and data subjects. BCRs must ensure that all employees who process personal data follow the privacy regulations of the jurisdictions where the data originates from, regardless of where they are located or where the data is transferred to.Reference: [Binding Corporate Rules], [BCRs for controllers], [BCRs for processors]

QUESTION 9
SCENARIO
Please use the following to answer the next QUESTION:
Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.
Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.
Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.
Richard believes that a transition from the use of fax machine to Internet faxing provides all of the following security benefits EXCEPT?

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

Correct Answer: A
Section:
Explanation:
A transition from the use of fax machine to Internet faxing does not provide the security benefit of greater accessibility to the faxes at an off-site location. This is because Internet faxing requires a secure internet connection and a compatible device to access the faxes online. If the user is at an off-site location that does not have these requirements, they may not be able to access their faxes. Furthermore, greater accessibility may not necessarily be a security benefit, as it may also increase the risk of unauthorized access or interception by third parties. Therefore, this option is not a security benefit of Internet faxing.
The other options are security benefits of Internet faxing. The ability to encrypt the transmitted faxes through a secure server ensures that the faxes are protected from eavesdropping or tampering during transmission. The reduction of the risk of data being seen or copied by unauthorized personnel eliminates the need for physical security measures such as locks or shredders for fax machines and paper documents.The ability to store faxes electronically, either on the user's PC or a password-protected network server, allows for better control and management of the faxes and reduces the storage space and costs associated with paper documents.Reference:1:Is Online Fax Secure in 2023? All You Need to Know!;2:Is faxing secure: How to fax from a computer safely - PandaDoc

QUESTION 10
SCENARIO
Please use the following to answer the next QUESTION:
Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.
Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal

data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.
Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.
As Richard begins to research more about Data Lifecycle Management (DLM), he discovers that the law office can lower the risk of a data breach by doing what?

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

Correct Answer: C
Section:
Explanation:
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 reducing the volume and the type of data that is stored in its system. This is because storing less data means having less data to protect and less data to lose in case of a breach.By reducing the volume and the type of data that is stored in its system, the law office can also comply with the data minimization principle under the GDPR and other data protection regulations, which requires that personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed3Therefore, this option is a way to lower the risk of a data breach.
The other options are not ways to lower the risk of a data breach by applying DLM principles. Prioritizing the data by order of importance may help to allocate resources and optimize performance, but it does not necessarily reduce the risk of a data breach. Minimizing the time it takes to retrieve the sensitive data may improve efficiency and responsiveness, but it does not necessarily reduce the risk of a data breach.Increasing the number of experienced staff to code and categorize the incoming data may enhance data quality and accuracy, but it does not necessarily reduce the risk of a data breach.Reference:3:Article 5 GDPR | General Data Protection Regulation (GDPR);4:Data Lifecycle Management: A Complete Guide | Splunk

QUESTION 11
SCENARIO
Please use the following to answer the next QUESTION:
Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.
Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.
Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.
Which of the following policy statements needs additional instructions in order to further protect the personal data of their clients?

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

Correct Answer: B
Section:
Explanation:
The policy statement that needs additional instructions in order to further protect the personal data of their clients is: All unused copies, prints, and faxes must be discarded in a designated recycling bin located near the work station and emptied daily. This policy statement is insufficient because it does not specify how the unused copies, prints, and faxes should be discarded. Simply throwing them into a recycling bin may expose them to

unauthorized access or theft by anyone who has access to the bin or its contents. Furthermore, emptying the bin daily may not be frequent enough to prevent accumulation or overflow of sensitive documents.
To further protect the personal data of their clients, this policy statement should include additional instructions such as:
All unused copies, prints, and faxes must be shredded before being discarded in a designated recycling bin located near the work station.
The recycling bin must be locked or secured at all times when not in use.
The recycling bin must be emptied at least twice a day or whenever it is full.
These additional instructions would ensure that the unused copies, prints, and faxes are destroyed in a secure manner and that the recycling bin is not accessible to unauthorized persons or prone to overflow.
The other policy statements do not need additional instructions, as they already provide adequate measures to protect the personal data of their clients. Documenting and double-checking the phone number for faxes ensures that the faxes are sent to the correct and intended recipient. Deleting the hard drives of copiers, printers, or fax machines before replacing or reselling them prevents data leakage or recovery by third parties. Not leaving the information visible on the computer screen and retrieving the printed document immediately prevents data exposure or theft by anyone who can see the screen or access the printer.

QUESTION 12
SCENARIO
Please use the following to answer the next QUESTION:
Richard McAdams recently graduated law school and decided to return to the small town of Lexington, Virginia to help run his aging grandfather's law practice. The elder McAdams desired a limited, lighter role in the practice, with the hope that his grandson would eventually take over when he fully retires. In addition to hiring Richard, Mr. McAdams employs two paralegals, an administrative assistant, and a part-time IT specialist who handles all of their basic networking needs. He plans to hire more employees once Richard gets settled and assesses the office's strategies for growth.
Immediately upon arrival, Richard was amazed at the amount of work that needed to done in order to modernize the office, mostly in regard to the handling of clients' personal data. His first goal is to digitize all the records kept in file cabinets, as many of the documents contain personally identifiable financial and medical data. Also, Richard has noticed the massive amount of copying by the administrative assistant throughout the day, a practice that not only adds daily to the number of files in the file cabinets, but may create security issues unless a formal policy is firmly in place Richard is also concerned with the overuse of the communal copier/ printer located in plain view of clients who frequent the building. Yet another area of concern is the use of the same fax machine by all of the employees. Richard hopes to reduce its use dramatically in order to ensure that personal data receives the utmost security and protection, and eventually move toward a strict Internet faxing policy by the year's end.
Richard expressed his concerns to his grandfather, who agreed, that updating data storage, data security, and an overall approach to increasing the protection of personal data in all facets is necessary Mr. McAdams granted him the freedom and authority to do so. Now Richard is not only beginning a career as an attorney, but also functioning as the privacy officer of the small firm. Richard plans to meet with the IT employee the following day, to get insight into how the office computer system is currently set-up and managed.
Richard needs to closely monitor the vendor in charge of creating the firm's database mainly because of what?

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

Correct Answer: D
Section:
Explanation:
The main reason why Richard needs to closely monitor the vendor in charge of creating the firm's database is that the vendor will be in direct contact with all of the law firm's personal data. This means that the vendor will have access to sensitive and confidential information about the law firm's clients, such as their financial and medical data, which could expose them to identity theft, fraud, or other harms if mishandled or breached.
Therefore, Richard needs to ensure that the vendor follows the best practices of data protection and security, such as:
Signing a data processing agreement that specifies the scope, purpose, duration, and terms of the data processing activities, as well as the rights and obligations of both parties.
Implementing appropriate technical and organizational measures to protect the data from unauthorized or unlawful access, use, disclosure, alteration, or destruction, such as encryption, access control, backup and recovery, logging and monitoring, etc.
Complying with the relevant laws and regulations that govern the collection, use, transfer, and retention of personal data, such as the GDPR or other local privacy laws.
Reporting any data breaches or incidents to the law firm and the relevant authorities as soon as possible and taking corrective actions to mitigate the impact and prevent recurrence.
Deleting or returning the data to the law firm after the completion of the project or upon request.

QUESTION 13
SCENARIO
Please use the following to answer the next QUESTION:
Amira is thrilled about the sudden expansion of NatGen. As the joint Chief Executive Officer (CEO) with her long-time business partner Sadie, Amira has watched the company grow into a major competitor in the green energy market. The current line of products includes wind turbines, solar energy panels, and equipment for geothermal systems. A talented team of developers means that NatGen's line of products will only continue to grow.

With the expansion, Amira and Sadie have received advice from new senior staff members brought on to help manage the company's growth. One recent suggestion has been to combine the legal and security functions of the company to ensure observance of privacy laws and the company's own privacy policy. This sounds overly complicated to Amira, who wants departments to be able to use, collect, store, and dispose of customer data in ways that will best suit their needs. She does not want administrative oversight and complex structuring to get in the way of people doing innovative work.
Sadie has a similar outlook. The new Chief Information Officer (CIO) has proposed what Sadie believes is an unnecessarily long timetable for designing a new privacy program. She has assured him that NatGen will use the best possible equipment for electronic storage of customer and employee data. She simply needs a list of equipment and an estimate of its cost. But the CIO insists that many issues are necessary to consider before the company gets to that stage.
Regardless, Sadie and Amira insist on giving employees space to do their jobs. Both CEOs want to entrust the monitoring of employee policy compliance to low-level managers. Amira and Sadie believe these managers can adjust the company privacy policy according to what works best for their particular departments. NatGen's CEOs know that flexible interpretations of the privacy policy in the name of promoting green energy would be highly unlikely to raise any concerns with their customer base, as long as the data is always used in course of normal business activities.
Perhaps what has been most perplexing to Sadie and Amira has been the CIO's recommendation to institute a privacy compliance hotline. Sadie and Amira have relented on this point, but they hope to compromise by allowing employees to take turns handling reports of privacy policy violations. The implementation will be easy because the employees need no special preparation. They will simply have to document any concerns they hear. Sadie and Amira are aware that it will be challenging to stay true to their principles and guard against corporate culture strangling creativity and employee morale. They hope that all senior staff will see the benefit of trying a unique approach.
If Amira and Sadie's ideas about adherence to the company's privacy policy go unchecked, the Federal Communications Commission (FCC) could potentially take action against NatGen for what?

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

Correct Answer: A
Section:
Explanation:
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 deceptive practices. This is because the FCC has the authority to enforce Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts or practices in or affecting commerce. By allowing different departments to use, collect, store, and dispose of customer data in ways that may not be consistent with the company's privacy policy, NatGen may be misleading its customers about how their personal information is protected and used. This could violate the FTC Act and expose NatGen to enforcement actions, fines, and reputational damage.Reference: [FCC Enforcement], [FTC Act], [Privacy Policy]

QUESTION 14
SCENARIO
Please use the following to answer the next QUESTION:
Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.
Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her ''I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?'' He has also told her that he works with a number of small companies that help him get projects completed in a hurry. ''We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have.''
In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team ''didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end.'' Penny is concerned that these issues will compromise Ace Space's privacy and data protection.
Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data ''shake up''. Her mission is to cultivate a strong privacy culture within the company.
Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.
To help Penny and her CEO with their objectives, what would be the most helpful approach to address her IT concerns?

A. Roll out an encryption policy
B. Undertake a tabletop exercise

C. Ensure inventory of IT assets is maintained
D. Host a town hall discussion for all IT employees

Correct Answer: B
Section:
Explanation:
The most helpful approach to address Penny's IT concerns is to undertake a tabletop exercise. A tabletop exercise is a simulated scenario that tests the organization's ability to respond to a security incident, such as a data breach, a cyberattack, or a malware infection. A tabletop exercise typically involves:
A facilitator who guides the participants through the scenario and injects additional challenges or variables
A scenario that describes a plausible security incident based on real-world threats or past incidents
A set of objectives that define the expected outcomes and goals of the exercise
A set of questions that prompt the participants to discuss their roles, responsibilities, actions, decisions, and communications during the incident response process
A feedback mechanism that collects the participants' opinions and suggestions on how to improve the incident response plan and capabilities
A tabletop exercise can help Penny and her CEO with their objectives by:
Enhancing the awareness and skills of the IT team and other stakeholders involved in incident response
Identifying and addressing the gaps, weaknesses, and challenges in the incident response plan and process
Improving the coordination and collaboration among the IT team and other stakeholders during incident response
Evaluating and validating the effectiveness and efficiency of the incident response plan and process
Generating and implementing lessons learned and best practices for incident response

QUESTION 15
SCENARIO
Please use the following to answer the next QUESTION:
For 15 years, Albert has worked at Treasure Box -- a mail order company in the United States (U.S.) that used to sell decorative candles around the world, but has recently decided to limit its shipments to customers in the 48 contiguous states. Despite his years of experience, Albert is often overlooked for managerial positions. His frustration about not being promoted, coupled with his recent interest in issues of privacy protection, have motivated Albert to be an agent of positive change.
He will soon interview for a newly advertised position, and during the interview, Albert plans on making executives aware of lapses in the company's privacy program. He feels certain he will be rewarded with a promotion for preventing negative consequences resulting from the company's outdated policies and procedures.
For example, Albert has learned about the AICPA (American Institute of Certified Public Accountants)/CICA (Canadian Institute of Chartered Accountants) Privacy Maturity Model (PMM). Albert thinks the model is a useful way to measure Treasure Box's ability to protect personal data. Albert has noticed that Treasure Box fails to meet the requirements of the highest level of maturity of this model; at his interview, Albert will pledge to assist the company with meeting this level in order to provide customers with the most rigorous security available.
Albert does want to show a positive outlook during his interview. He intends to praise the company's commitment to the security of customer and employee personal data against external threats. However, Albert worries about the high turnover rate within the company, particularly in the area of direct phone marketing. He sees many unfamiliar faces every day who are hired to do the marketing, and he often hears complaints in the lunch room regarding long hours and low pay, as well as what seems to be flagrant disregard for company procedures.
In addition, Treasure Box has had two recent security incidents. The company has responded to the incidents with internal audits and updates to security safeguards. However, profits still seem to be affected and anecdotal evidence indicates that many people still harbor mistrust. Albert wants to help the company recover. He knows there is at least one incident the public 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

Correct Answer: B

Section:
Explanation:
This answer is the best way to describe the handling procedure that Albert suggests and that may help the company to earn back the trust of its customer base, as it involves creating a toll-free number for customers, as well as a more efficient procedure for responding to customer concerns by postal mail. Correction is a handling procedure that allows customers to request that the company updates, modifies or deletes their personal data if it is inaccurate, incomplete or outdated. Correction can help to enhance the quality and integrity of the data, as well as to respect the rights and preferences of the customers. Correction can also help to improve the customer satisfaction and loyalty, as well as to prevent or reduce any errors or disputes that may arise from incorrect or outdated data.

QUESTION 16
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.

Correct Answer: D
Section:
Explanation:
In regards to the collection of personal data conducted by an organization, the data subject must be allowed to challenge the authenticity of the personal data and have it corrected if needed.This is a fundamental right of data subjects under various data protection laws and regulations, such as the EU General Data Protection Regulation (GDPR)1, the California Consumer Privacy Act (CCPA)2, and the Personal Data Protection Act (PDPA) of Singapore3. This right enables data subjects to verify the accuracy and completeness of their personal data and to request rectification or erasure of any inaccurate or incomplete data. This right also helps organizations to maintain high standards of data quality and integrity.

QUESTION 17
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.

Correct Answer: A
Section:
Explanation:
A Privacy Impact Assessment (PIA) is a process that helps to identify and mitigate the privacy risks of a project or activity that involves personal data. A PIA is usually required when there is a new or significant change in the way personal data is collected, used, or disclosed. Therefore, a PIA would be the least likely to be required if a company created a credit-scoring platform five years ago, as this would not be a new or significant change. The other situations involve new or changed processing of personal data that could have privacy impacts, such as sensitive data (health or children's data), profiling data (user profiles), or large-scale data (patient's file).Reference:CIPM Study Guide, page 30;Guide to undertaking privacy impact assessments.

QUESTION 18
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.

Correct Answer: D

Section:
Explanation:
Under the GDPR, a written agreement between the controller and processor must include an obligation on the processor to assist the controller in complying with the controller's obligations to notify the supervisory authority and the data subjects about personal data breaches.This is stated in Article 28(3)(f) of the GDPR1. The other options are not required by the GDPR, although they may be included in the agreement as additional clauses.The obligation to report any personal data breach to the controller within 72 hours is imposed on the processor by Article 33(2) of the GDPR1, not by the agreement.The obligation to report any serious personal data breach to the supervisory authority is imposed on the controller by Article 33(1) of the GDPR1, not by the agreement. The termination of the agreement in case of a personal data breach is not a mandatory provision under the GDPR, but rather a contractual matter that may depend on the circumstances and severity of the breach.Reference:GDPR

QUESTION 19
SCENARIO
Please use the following to answer the next QUESTION:
Perhaps Jack Kelly should have stayed in the U.S. He enjoys a formidable reputation inside the company, Special Handling Shipping, for his work in reforming certain 'rogue' offices. Last year, news broke that a police sting operation had revealed a drug ring operating in the Providence, Rhode Island office in the United States. Video from the office's video surveillance cameras leaked to news operations showed a drug exchange between Special Handling staff and undercover officers.
In the wake of this incident, Kelly had been sent to Providence to change the 'hands off' culture that upper management believed had let the criminal elements conduct their illicit transactions. After a few weeks under Kelly's direction, the office became a model of efficiency and customer service. Kelly monitored his workers' activities using the same cameras that had recorded the illegal conduct of their former co-workers.
Now Kelly has been charged with turning around the office in Cork, Ireland, another trouble spot. The company has received numerous reports of the staff leaving the office unattended. When Kelly arrived, he found that even when present, the staff often spent their days socializing or conducting personal business on their mobile phones. Again, he observed their behaviors using surveillance cameras. He issued written reprimands to six staff members based on the first day of video alone.
Much to Kelly's surprise and chagrin, he and the company are now under investigation by the Data Protection Commissioner of Ireland for allegedly violating the privacy rights of employees. Kelly was told that the company's license for the cameras listed facility security as their main use, but he does not know why this matters. He has pointed out to his superiors that the company's training programs on privacy protection and data collection mention nothing about surveillance video.
You are a privacy protection consultant, hired by the company to assess this incident, report on the legal and compliance issues, and recommend next steps.
What does this example best illustrate about training requirements for privacy protection?

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

Correct Answer: B
Section:
Explanation:
This answer is the best way to illustrate the training requirements for privacy protection, as it shows the importance of understanding and complying with the different legal and regulatory frameworks that apply to the organization's data processing activities in different jurisdictions. Training on local laws must be implemented for all personnel who are involved in or responsible for collecting, using, disclosing, storing or transferring personal data across borders, as they may face different obligations and restrictions depending on the nature and location of the data and the data subjects.Training on local laws can help to prevent or mitigate the risks of violating the privacy rights of individuals, facing legal actions, fines, sanctions or investigations from authorities, or losing trust and reputation among customers, partners and stakeholders.Reference: IAPP CIPM Study Guide, page 901; ISO/IEC 27002:2013, section 7.2.2

QUESTION 20
SCENARIO
Please use the following to answer the next QUESTION:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. 'It's going to be great,' the developer, Deidre Hoffman, tells you, 'if, that is, we actually get it working!' She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. 'It's just three young people,' she says, 'but they do

great work.' She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. 'They do good work, so I chose them.'
Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, 'I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!'
You want to point out that normal protocols have NOT been followed in this matter. Which process in particular has been neglected?

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

Correct Answer: D
Section:
Explanation:
This answer is the best way to point out that normal protocols have not been followed in this matter, as it shows that the vendor selection process was not conducted properly and that the vendor's privacy and security practices were not assessed or verified before engaging them for the app development project. Vendor due diligence vetting is a process that involves evaluating and comparing potential vendors based on their qualifications, capabilities, reputation, experience, performance and compliance with the organization's standards and expectations, as well as the applicable laws and regulations. Vendor due diligence vetting can help to ensure that the vendor can deliver the project on time, on budget and on quality, as well as protect the personal data that they process on behalf of the organization.Vendor due diligence vetting can also help to identify and mitigate any risks or issues that may arise from the vendor relationship, such as data breaches, legal actions, fines, sanctions or investigations.Reference: IAPP CIPM Study Guide, page 821; ISO/IEC 27002:2013, section 15.1.1

QUESTION 21
SCENARIO
Please use the following to answer the next QUESTION:
Edufox has hosted an annual convention of users of its famous e-learning software platform, and over time, it has become a grand event. It fills one of the large downtown conference hotels and overflows into the others, with several thousand attendees enjoying three days of presentations, panel discussions and networking. The convention is the centerpiece of the company's product rollout schedule and a great training opportunity for current users. The sales force also encourages prospective clients to attend to get a better sense of the ways in which the system can be customized to meet diverse needs and understand that when they buy into this system, they are joining a community that feels like family.
This year's conference is only three weeks away, and you have just heard news of a new initiative supporting it: a smartphone app for attendees. The app will support late registration, highlight the featured presentations and provide a mobile version of the conference program. It also links to a restaurant reservation system with the best cuisine in the areas featured. 'It's going to be great,' the developer, Deidre Hoffman, tells you, 'if, that is, we actually get it working!' She laughs nervously but explains that because of the tight time frame she'd been given to build the app, she outsourced the job to a local firm. 'It's just three young people,' she says, 'but they do great work.' She describes some of the other apps they have built. When asked how they were selected for this job, Deidre shrugs. 'They do good work, so I chose them.'
Deidre is a terrific employee with a strong track record. That's why she's been charged to deliver this rushed project. You're sure she has the best interests of the company at heart, and you don't doubt that she's under pressure to meet a deadline that cannot be pushed back. However, you have concerns about the app's handling of personal data and its security safeguards. Over lunch in the break room, you start to talk to her about it, but she quickly tries to reassure you, 'I'm sure with your help we can fix any security issues if we have to, but I doubt there'll be any. These people build apps for a living, and they know what they're doing. You worry too much, but that's why you're so good at your job!'
You see evidence that company employees routinely circumvent the privacy officer in developing new initiatives.
How can you best draw attention to the scope of this problem?

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

Correct Answer: B
Section:
Explanation:
This answer is the best way to draw attention to the scope of this problem, as it can provide quantitative and objective evidence of how often the privacy officer is bypassed or ignored in the organization's data processing activities. Developing a metric showing the number of initiatives launched without consultation can help to measure and monitor the level of compliance and alignment with the organization's privacy program and policies, as

well as the applicable laws and regulations. Including this metric in reports, presentations and consultation can help to communicate and raise awareness of this problem among the relevant stakeholders, such as senior management, project managers, developers or vendors.It can also help to demonstrate the value and importance of involving the privacy officer in the early stages of any initiative that involves personal data, as well as the potential consequences and risks of not doing so.Reference: IAPP CIPM Study Guide, page 891; ISO/IEC 27002:2013, section 18.1.3

QUESTION 22
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.

Correct Answer: C
Section:
Explanation:
The GDPR imposes several obligations on data processors, such as maintaining records of processing activities, cooperating with supervisory authorities, and notifying data controllers of personal data breaches. One of these obligations is to implement appropriate technical and organizational measures that ensure an appropriate level of security for the personal data processed on behalf of the data controller.This is stated in Article 28(1) and Article 32 of the GDPR1. The other options are not obligations of data processors under the GDPR, but rather of data controllers or joint responsibilities of both parties.Reference:GDPR

QUESTION 23
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.

Correct Answer: B
Section:
Explanation:
Industry frameworks are the most effective resource for an executive who wants to develop her company's privacy program beyond what is specifically required by law. Industry frameworks are collections of best practices, standards, and guidelines that help organizations establish and improve their privacy policies and procedures. Industry frameworks can help organizations demonstrate their commitment to privacy, enhance their reputation and trustworthiness, and comply with multiple privacy regulations.Some examples of industry frameworks are the NIST Privacy Framework2, the ISO 27701 Privacy Information Management System3, and the AICPA/CICA Generally Accepted Privacy Principles (GAPP)4. The other options are not as effective as industry frameworks for developing a privacy program. Internal auditors can help evaluate the effectiveness and compliance of existing privacy controls, but they may not provide guidance on how to improve or expand them. Oversight organizations can enforce privacy laws and regulations, but they may not offer advice on how to go beyond the legal requirements. Breach notifications from competitors can alert organizations to potential threats and vulnerabilities, but they may not suggest how to prevent or mitigate them.Reference:NIST Privacy Framework;ISO 27701 Privacy Information Management System;AICPA/CICA Generally Accepted Privacy Principles (GAPP)

QUESTION 24
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.

Correct Answer: D

Section:
Explanation:
One reason the European Union has enacted more comprehensive privacy laws than the United States is to allow the free movement of data between member countries. The EU considers data protection as a fundamental right that applies to all individuals within its territory, regardless of their nationality or residence.The EU has adopted a harmonized legal framework for data protection, such as the GDPR1and the ePrivacy Directive5, that applies to all member states and ensures a consistent level of protection across the EU. The EU also requires that any transfers of personal data outside the EU are subject to adequate safeguards or exceptions that guarantee an equivalent level of protection. The EU's approach to data protection aims to facilitate the internal market and promote economic and social integration among member states by removing barriers and restrictions to the cross-border flow of data. The other options are not reasons why the EU has enacted more comprehensive privacy laws than the US. The EU does not necessarily have more adequate enforcement or funding for its privacy laws than the US, although it does have a network of independent supervisory authorities that monitor and enforce compliance with the EU data protection rules. The EU does not allow separate industries to set privacy standards, but rather imposes uniform and binding rules for all sectors and activities that involve personal data processing.Reference:GDPR;ePrivacy Directive

QUESTION 25
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.

Correct Answer: D
Section:
Explanation:
All of the changes listed will likely trigger a data inventory update except for the passage of a new privacy regulation. A data inventory is a record of all personal data that an organization collects, processes, stores, shares, or disposes of. A data inventory helps an organization understand what types of personal data it holds, where it comes from, where it goes, and how it is protected. A data inventory should be updated regularly to reflect any changes in the organization's data processing activities or practices. Some examples of changes that would trigger a data inventory update are outsourcing a business function, acquiring a new subsidiary, or onboarding a new vendor. These changes may involve new sources or destinations of personal data, new purposes or categories of processing, new security measures or risks, or new contractual agreements or obligations. The passage of a new privacy regulation may not trigger a data inventory update unless it affects the organization's existing data processing activities or practices. However, it may trigger a compliance assessment or gap analysis to determine if the organization needs to make any adjustments to its privacy program or policies to meet the new legal requirements.Reference:Data Inventory Hub;Data Inventory: What It Is & How To Create One

QUESTION 26
SCENARIO
Please use the following to answer the next QUESTION:
Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. 'Carlton won't listen to me,' Paul says, 'but he may pay attention to an expert.'
Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks. espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. 'This is a technology company,' Carlton says. 'We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts.'
The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A 'cleaning crew' of one teenager is emptying the trash bins. A few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: 'Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!'
What would be the best kind of audit to recommend for Gadgo?

A. A supplier audit.
B. An internal audit.
C. A third-party audit.
D. A self-certification.

Correct Answer: C
Section:

Explanation:
This answer is the best kind of audit to recommend for Gadgo, as it can provide an independent and objective assessment of the company's privacy program and practices, as well as identify any gaps, weaknesses or risks that need to be addressed or improved. A third-party audit is conducted by an external auditor who has the necessary expertise, experience and credentials to evaluate the company's compliance with the applicable laws, regulations, standards and best practices for data protection.A third-party audit can also help to enhance the company's reputation and trust among its customers, partners and stakeholders, as well as demonstrate its commitment and accountability for privacy protection.Reference: IAPP CIPM Study Guide, page 881; ISO/IEC 27002:2013, section 18.2.1

QUESTION 27
SCENARIO
Please use the following to answer the next QUESTION:
Paul Daniels, with years of experience as a CEO, is worried about his son Carlton's successful venture, Gadgo. A technological innovator in the communication industry that quickly became profitable, Gadgo has moved beyond its startup phase. While it has retained its vibrant energy, Paul fears that under Carlton's direction, the company may not be taking its risks or obligations as seriously as it needs to. Paul has hired you, a Privacy Consultant, to assess the company and report to both father and son. 'Carlton won't listen to me,' Paul says, 'but he may pay attention to an expert.'
Gadgo's workplace is a clubhouse for innovation, with games, toys, snacks. espresso machines, giant fish tanks and even an iguana who regards you with little interest. Carlton, too, seems bored as he describes to you the company's procedures and technologies for data protection. It's a loose assemblage of controls, lacking consistency and with plenty of weaknesses. 'This is a technology company,' Carlton says. 'We create. We innovate. I don't want unnecessary measures that will only slow people down and clutter their thoughts.'
The meeting lasts until early evening. Upon leaving, you walk through the office it looks as if a strong windstorm has recently blown through, with papers scattered across desks and tables and even the floor. A 'cleaning crew' of one teenager is emptying the trash bins. A few computers have been left on for the night, others are missing. Carlton takes note of your attention to this: 'Most of my people take their laptops home with them, or use their own tablets or phones. I want them to use whatever helps them to think and be ready day or night for that great insight. It may only come once!'
What phase in the Privacy Maturity Model (PMM) does Gadgo's privacy program best exhibit?

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

Correct Answer: A
Section:
Explanation:
This answer is the best way to describe the phase in the Privacy Maturity Model (PMM) that Gadgo's privacy program best exhibits, as it shows that the company has no formal or consistent approach to privacy protection and that its privacy practices are largely reactive, unplanned and uncoordinated. The ad hoc phase is the lowest level of maturity in the PMM, which is a framework that measures the effectiveness and maturity of an organization's privacy program based on five phases: ad hoc, repeatable, defined, managed and optimized.The ad hoc phase indicates that the organization has little or no awareness of its privacy obligations and risks, and that its privacy activities are dependent on individual efforts or initiatives, rather than on organizational policies or processes.Reference: IAPP CIPM Study Guide, page 891; ISO/IEC 27002:2013, section 18.1.1

QUESTION 28
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.

Correct Answer: C
Section:
Explanation:
This answer is the best form of trend analysis that Incipia Corporation should use to analyze the effectiveness of the training over the next six months, as it can provide a quantitative and objective way to measure and compare the results and outcomes of the training against predefined criteria or indicators. Statistical trend analysis is a method that involves collecting, analyzing and presenting data using statistical tools and techniques, such as charts, graphs, tables or formulas.Statistical trend analysis can help to identify patterns, changes or correlations in the data over time, as well as to evaluate the performance and impact of the training on the organization's privacy program and objectives.Reference: IAPP CIPM Study Guide, page 901; ISO/IEC 27002:2013, section 18.1.3

QUESTION 29
SCENARIO
Please use the following to answer the next QUESTION:
Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested
IgNight's installations in their homes across the globe.
One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.
Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.
To determine the steps to follow, what would be the most appropriate internal guide for Ben to review?

A. Incident Response Plan.
B. Code of Business Conduct.
C. IT Systems and Operations Handbook.
D. Business Continuity and Disaster Recovery Plan.

Correct Answer: A
Section:
Explanation:
The most appropriate internal guide for Ben to review is the Incident Response Plan. An Incident Response Plan is a document that outlines how an organization will respond to a security incident, such as a data breach, a cyberattack, or a malware infection. An Incident Response Plan typically includes:
The roles and responsibilities of the incident response team and other stakeholders
The procedures and protocols for detecting, containing, analyzing, and resolving incidents
The communication and escalation channels for reporting and notifying incidents
The tools and resources for conducting incident response activities
The criteria and methods for evaluating and improving the incident response process
An Incident Response Plan helps an organization prepare for and deal with security incidents in an effective and efficient manner. It also helps an organization minimize the impact and damage of security incidents, comply with legal and regulatory obligations, and restore normal operations as soon as possible.
The other options are not as relevant or useful as the Incident Response Plan for Ben's situation. The Code of Business Conduct is a document that defines the ethical standards and expectations for the organization's employees and stakeholders. It may include some general principles or policies related to security, but it does not provide specific guidance on how to handle security incidents. The IT Systems and Operations Handbook is a document that describes the technical aspects and functions of the organization's IT systems and infrastructure. It may include some information on security controls and configurations, but it does not provide detailed instructions on how to perform incident response tasks. The Business Continuity and Disaster Recovery Plan is a document that outlines how an organization will continue its critical functions and operations in the event of a disruption or disaster, such as a natural disaster, a power outage, or a fire. It may include some measures to protect or recover data and systems, but it does not focus on security incidents or threats.Reference:What Is an Incident Response Plan for IT?;Incident Response Plan (IRP) Basics

QUESTION 30
SCENARIO
Please use the following to answer the next QUESTION:
Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.
One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.
Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.
If this were a data breach, how is it likely to be categorized?

A. Availability Breach.
B. Authenticity Breach.
C. Confidentiality Breach.
D. Integrity Breach.

Correct Answer: C
Section:
Explanation:
If this were a data breach, it is likely to be categorized as a confidentiality breach. A confidentiality breach is a type of data breach that involves unauthorized or accidental disclosure of or access to personal data. A confidentiality breach violates the principle of confidentiality, which requires that personal data is protected from unauthorized or unlawful use or disclosure. A confidentiality breach can occur when personal data is exposed to unauthorized parties, such as hackers, competitors, or third parties without consent. A confidentiality breach can also occur when personal data is sent to incorrect recipients, such as by email or mail.
The other options are not likely to be the correct category for this data breach. An availability breach is a type of data breach that involves accidental or unauthorized loss of access to or destruction of personal data. An availability breach violates the principle of availability, which requires that personal data is accessible and usable by authorized parties when needed. An availability breach can occur when personal data is deleted, corrupted, encrypted, or otherwise rendered inaccessible by malicious actors or technical errors. An authenticity breach is a type of data breach that involves unauthorized or accidental alteration of personal data. An authenticity breach violates the principle of authenticity, which requires that personal data is accurate and up to date. An authenticity breach can occur when personal data is modified, tampered with, or falsified by malicious actors or human errors. An integrity breach is a type of data breach that involves unauthorized or accidental alteration of personal data that affects its quality or reliability. An integrity breach violates the principle of integrity, which requires that personal data is complete and consistent with its intended purpose. An integrity breach can occur when personal data is incomplete, inconsistent, outdated, or inaccurate due to malicious actors or human errors.Reference:Personal Data Breaches: A Guide;Guidance on the Categorisation and Notification of Personal Data Breaches

QUESTION 31
SCENARIO
Please use the following to answer the next QUESTION:
Ben works in the IT department of IgNight, Inc., a company that designs lighting solutions for its clients. Although IgNight's customer base consists primarily of offices in the US, some individuals have been so impressed by the unique aesthetic and energy-saving design of the light fixtures that they have requested IgNight's installations in their homes across the globe.
One Sunday morning, while using his work laptop to purchase tickets for an upcoming music festival, Ben happens to notice some unusual user activity on company files. From a cursory review, all the data still appears to be where it is meant to be but he can't shake off the feeling that something is not right. He knows that it is a possibility that this could be a colleague performing unscheduled maintenance, but he recalls an email from his company's security team reminding employees to be on alert for attacks from a known group of malicious actors specifically targeting the industry.
Ben is a diligent employee and wants to make sure that he protects the company but he does not want to bother his hard-working colleagues on the weekend. He is going to discuss the matter with this manager first thing in the morning but wants to be prepared so he can demonstrate his knowledge in this area and plead his case for a promotion.
Going forward, what is the best way for IgNight to prepare its IT team to manage these kind of security events?

A. Tabletop exercises.
B. Update its data inventory.
C. IT security awareness training.
D. Share communications relating to scheduled maintenance.

Correct Answer: A
Section:
Explanation:
The best way for IgNight to prepare its IT team to manage these kind of security events is to conduct tabletop exercises. Tabletop exercises are simulated scenarios that test the organization's ability to respond to security incidents in a realistic and interactive way. Tabletop exercises typically involve:
A facilitator who guides the participants through the scenario and injects additional challenges or variables
A scenario that describes a plausible security incident based on real-world threats or past incidents
A set of objectives that define the expected outcomes and goals of the exercise
A set of questions that prompt the participants to discuss their roles, responsibilities, actions, decisions, and communications during the incident response process
A feedback mechanism that collects the participants' opinions and suggestions on how to improve the incident response plan and capabilities
Tabletop exercises help an organization prepare for and deal with security incidents by:
Enhancing the awareness and skills of the IT team and other stakeholders involved in incident response
Identifying and addressing the gaps, weaknesses, and challenges in the incident response plan and process

Improving the coordination and collaboration among the IT team and other stakeholders during incident response
Evaluating and validating the effectiveness and efficiency of the incident response plan and process
Generating and implementing lessons learned and best practices for incident response
The other options are not as effective or useful as tabletop exercises for preparing the IT team to manage security events. Updating the data inventory is a good practice for maintaining an accurate and comprehensive record of the personal data that the organization collects, processes, stores, shares, or disposes of. However, it does not test or improve the organization's incident response capabilities or readiness. IT security awareness training is a good practice for educating the IT team and other employees on the basic principles and practices of cybersecurity. However, it does not simulate or replicate the real-world situations and challenges that the IT team may face during security incidents. Sharing communications relating to scheduled maintenance is a good practice for informing the IT team and other stakeholders of the planned activities and potential impacts on the IT systems and infrastructure. However, it does not prepare the IT team for dealing with unplanned or unexpected security events that may require immediate and coordinated response.Reference:CISA Tabletop Exercise Packages;Cybersecurity Tabletop Exercise Examples, Best Practices, and Considerations;Six Tabletop Exercises to Help Prepare Your Cybersecurity Team

QUESTION 32
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.

Correct Answer: D
Section:
Explanation:
The creation of the business case is the first step in privacy framework development, as it helps to identify the individual program needs and specific organizational goals. The business case is a document that outlines the rationale, objectives, benefits, costs, risks, and alternatives for implementing a privacy program. It also helps to communicate the value of privacy to stakeholders and gain their support. The other options are subsequent steps in privacy framework development, after the business case has been established.Reference:CIPM Study Guide, page 15.

QUESTION 33
SCENARIO
Please use the following to answer the next QUESTION:
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.

Correct Answer: B
Section:
Explanation:
This answer is the most realistic step the organization can take to help diminish liability in the event of another incident, as it can ensure that the vendor complies with the same standards and obligations as the organization regarding data protection. Vendor contracts should include clauses that specify the scope, purpose, duration and type of data processing, as well as the rights and responsibilities of both parties. The contracts should also require the vendor to implement appropriate technical and organizational measures to protect the data from unauthorized or unlawful access, use, disclosure, alteration or destruction, and to notify the organization of any security incidents or breaches. The contracts should also allow the organization to monitor, audit or inspect the vendor's performance and compliance with the contract terms and applicable laws and regulations.Reference: IAPP CIPM Study Guide, page 82; ISO/IEC 27002:2013, section 15.1.2

QUESTION 34
SCENARIO
Please use the following to answer the next QUESTION:
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.

Correct Answer: A
Section:
Explanation:
This answer is the best way to create better employee awareness of the company's privacy program, as it can increase the effectiveness and retention of the information by appealing to different learning styles and preferences. Varying the modes of communication can include using different formats and channels, such as posters, emails, memos, videos, webinars, podcasts, newsletters, quizzes, games or interactive modules. Varying the modes of communication can also help to avoid information overload or duplication, which may cause employees to ignore or disregard the privacy messages.Reference: IAPP CIPM Study Guide, page 90; ISO/IEC 27002:2013, section 7.2.2

QUESTION 35
SCENARIO
Please use the following to answer the next QUESTION:
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.

Correct Answer: B
Section:
Explanation:
This answer is the best way to address the objection to Spencer's training suggestion, as it can provide flexibility and convenience for employees who work in different locations or have different schedules. Alternative delivery methods for trainings can include online courses, webinars, podcasts, videos or self-paced modules that can be accessed anytime and anywhere by employees. Alternative delivery methods can also reduce the cost and time required for in-person trainings, while still ensuring that employees receive consistent and relevant information on the company's privacy program.Reference: IAPP CIPM Study Guide, page 90; ISO/IEC 27002:2013, section 7.2.2

QUESTION 36
SCENARIO
Please use the following to answer the next QUESTION:
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.

Correct Answer: A
Section:
Explanation:
Spencer has a misconception regarding the amount of responsibility that a data controller retains, as he suggests that the contractors should be held contractually liable for telling customers about any security incidents, and that Nationwide Grill should not be forced to soil the company name for a problem it did not cause. However, as a data controller, Nationwide Grill is ultimately responsible for ensuring that the personal data of its customers is processed in compliance with applicable laws and regulations, regardless of whether it uses contractors or not. Nationwide Grill cannot transfer or delegate its accountability or liability to the contractors, and it has a duty to inform the customers and the relevant authorities of any security incidents or breaches that may affect their data. Therefore, Spencer's view is unrealistic and risky, as it may expose Nationwide Grill to legal actions, fines, reputational damage and loss of trust.

QUESTION 37
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.

Correct Answer: C
Section:
Explanation:
Rationalizing requirements is an organizational approach that involves identifying and harmonizing the common elements of different privacy regulations and standards. This can make compliance easier and more efficient, as well as reduce the risk of conflicts or gaps in privacy protection. Rationalizing requirements can also help to create a consistent privacy policy and culture across different jurisdictions and business units.Reference:CIPM Study Guide, page 23.

QUESTION 38
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.

Correct Answer: C
Section:
Explanation:
Limitations on liability are not a key consideration when implementing Privacy by Design (PbD). PbD is a methodology that aims to protect privacy by embedding it into the design of systems and data. The key considerations for PbD are based on seven principles that include collection limitation, data minimization, and purpose specification, among others. Limitations on liability are more relevant for contractual or legal aspects of privacy, not for design or engineering aspects.Reference:CIPM Study Guide, page 25;The 7 Principles of Privacy by Design.

QUESTION 39
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.

Correct Answer: A
Section:
Explanation:
The number of security patches applied to company devices might be the least relevant metric for a company's privacy and governance team after a data breach. While security patches are important for preventing future breaches, they do not directly measure the impact or response of the current breach. The other metrics are more relevant for assessing how the company handled the breach, such as how it complied with the privacy rights of affected individuals, how it evaluated the privacy risks of its systems, and how it trained its employees on data awareness.Reference:CIPM Study Guide, page 28.

QUESTION 40
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.

Correct Answer: C
Section:
Explanation:
The best way to understand the location, use and importance of personal data within an organization is by evaluating methods for collecting data. This will help to identify the sources, purposes, and categories of data that the organization processes, as well as the data flows and transfers within and outside the organization. By doing so, the organization can assess the risks and opportunities associated with data processing and design appropriate privacy policies and controls.Reference: [IAPP CIPM Study Guide], page 29-30; [Data Inventory]

QUESTION 41
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.

Correct Answer: A
Section:
Explanation:
If you succumb to ''overgeneralization'' when analyzing data from metrics, you are using data that is too broad to capture specific meanings. For example, if you use a single metric such as ''number of complaints'' to measure customer satisfaction, you are ignoring other factors that may affect customer satisfaction such as quality of service, responsiveness, or loyalty. You are also assuming that all complaints are equally valid and important, which may not be the case. To avoid overgeneralization, you should use multiple metrics that are relevant, specific, and measurable for your objectives.Reference: [IAPP CIPM Study Guide], page 59-60; [Avoiding Overgeneralization in Data Analysis]

QUESTION 42
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.

Correct Answer: D
Section:
Explanation:
In addition to regulatory requirements and business practices, an important factor that a global privacy strategy must consider is cultural norms. Different cultures may have different expectations and preferences regarding privacy, such as what constitutes personal information, how consent is obtained and expressed, how data is used and shared, and how privacy rights are enforced. A global privacy strategy should respect and accommodate these cultural differences and ensure that the organization's privacy practices are transparent, fair, and consistent across different regions.Reference: [IAPP CIPM Study Guide], page 81-82; [Cultural Differences in Privacy Expectations]

QUESTION 43
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.

Correct Answer: C
Section:
Explanation:
An important trend in privacy program development is the movement beyond crisis management to proactive prevention. This means that instead of reacting to privacy breaches or incidents after they occur, organizations are taking steps to prevent them from happening in the first place. This involves implementing privacy by design principles, conducting privacy impact assessments, adopting privacy-enhancing technologies, training staff on privacy awareness and best practices, and monitoring compliance and performance. By doing so, organizations can reduce risks, costs, and reputational damage associated with privacy violations.Reference: [IAPP CIPM Study Guide], page 93-94; [Moving from Crisis Management to Proactive Prevention]

QUESTION 44
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.
The packaging and user guide for the Handy Helper indicate that it is a 'privacy friendly' product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What step in the system development process did Manasa skip?

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

Correct Answer: B
Section:
Explanation:
Manasa skipped the step of working with Sanjay to review any necessary privacy requirements to be built into the product.This step is part of the system analysis phase, which is less theoretical and focuses more on practical application1By working with Sanjay, Manasa could have identified the legal and ethical obligations that Omnipresent Omnimedia has to protect the privacy of its users, especially in different jurisdictions.She could have also incorporated privacy by design principles, such as data minimization, purpose limitation, and user consent, into the product development process2This would have helped to avoid potential privacy risks and violations that could harm the reputation and trust of the company and its customers.Reference:1:7 Phases of the System Development Life Cycle (With Tips);2: [Privacy by Design: The 7 Foundational Principles]

QUESTION 45
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.
The packaging and user guide for the Handy Helper indicate that it is a 'privacy friendly' product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What administrative safeguards should be implemented to protect the collected data while in use by Manasa and her product management team?

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

Correct Answer: C
Section:
Explanation:
An administrative safeguard that should be implemented to protect the collected data while in use by Manasa and her product management team is a policy restricting data access on a ''need to know'' basis.This means that only authorized personnel who have a legitimate business purpose for accessing the data should be able to do so3This would help to prevent unauthorized or unnecessary access, use, or disclosure of sensitive or personal data by internal or external parties.It would also reduce the risk of data breaches, theft, or loss that could compromise the confidentiality, integrity, and availability of the data4Reference:3:HIPAA Security Series #2 - Administrative Safeguards - HHS.gov;4:Administrative Safeguards of the Security Rule: What Are They?

QUESTION 46
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.
The packaging and user guide for the Handy Helper indicate that it is a 'privacy friendly' product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to

look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What element of the Privacy by Design (PbD) framework might the Handy Helper violate?

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

Correct Answer: D
Section:
Explanation:
The Handy Helper might violate the element of the Privacy by Design (PbD) framework that requires integrating privacy throughout the system development life cycle.According to the PbD framework, privacy should be embedded into the design and architecture of IT systems and business practices, not added as an afterthought1This means that privacy should be considered at every stage of the system development life cycle, from planning to analysis to design to development to implementation to maintenance2However, the Handy Helper seems to have been developed without involving Sanjay, the head of privacy, or conducting a privacy impact assessment (PIA) to identify and mitigate potential privacy risks3The product also lacks a clear and transparent privacy notice that informs users about what data is collected, how it is used, where it is stored, who has access to it, and what choices they have4These issues could expose the product to legal and reputational challenges, especially in regions with strict data protection regulations, such as Europe.Reference:1:Privacy by Design - The LIFE Institute;2:System Development Life Cycle - GeeksforGeeks;3: [Privacy Impact Assessment (PIA) | NZ Digital government];4: [Privacy Notices under EU Data Protection Law | Privacy International]

QUESTION 47
SCENARIO
Please use the following to answer the next QUESTION:
Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.
The packaging and user guide for the Handy Helper indicate that it is a 'privacy friendly' product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.
Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.
In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.
Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.
What can Sanjay do to minimize the risks of offering the product in Europe?

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

Correct Answer: B
Section:
Explanation:

Sanjay should work with Manasa to review and remediate the Handy Helper as a gating item before it is released. This means that Sanjay should collaborate with Manasa and her product team to evaluate the privacy implications of the product and address any gaps or issues before launching it in Europe. This could involve conducting a PIA, applying the PbD principles, revising the consent mechanism, updating the privacy notice, ensuring compliance with data localization requirements, implementing data security measures, and limiting data access based on the least privilege principle. By doing so, Sanjay could help minimize the risks of offering the product in Europe and avoid potential violations of the General Data Protection Regulation (GDPR) or other local laws that could result in fines, lawsuits, or loss of trust.

QUESTION 48
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.

Correct Answer: C
Section:
Explanation:
The statement that is false regarding the use of technical security controls is that most privacy legislation lists the types of technical security controls that must be implemented.Technical security controls are the hardware and software components that protect a system against cyberattacks, such as encryption, firewalls, antivirus software, and access control mechanisms1However, most privacy legislation does not prescribe specific types of technical security controls that must be implemented by organizations.Instead, they usually require organizations to implement reasonable or appropriate technical security measures to protect personal data from unauthorized or unlawful access, use, disclosure, alteration, or destruction23The exact level and type of technical security controls may depend on various factors, such as the nature and sensitivity of the data, the risks and threats involved, the state of the art technology available, and the cost and feasibility of implementation4Therefore, organizations have some flexibility and discretion in choosing the most suitable technical security controls for their data processing activities.Reference:1:Technical Controls --- Cybersecurity Resilience - Resilient Energy Platform;2: [General Data Protection Regulation (GDPR) -- Official Legal Text], Article 32;3: [Privacy Act 1988], Schedule 1 - Australian Privacy Principles (APPs), APP 11;4:Technical Security Controls: Encryption, Firewalls & More

QUESTION 49
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.

Correct Answer: A
Section:
Explanation:
The first action that the privacy officer should take after being notified by the benefits manager that she accidentally sent out the retirement enrollment report of all employees to a wrong vendor is to perform a risk of harm analysis.A risk of harm analysis is a process of assessing the potential adverse consequences for the individuals whose personal data has been compromised by a data breach or incident5The purpose of this analysis is to determine whether the breach or incident poses a significant risk of harm to the affected individuals, such as identity theft, fraud, discrimination, physical harm, emotional distress, or reputational damage6The risk of harm analysis should consider various factors, such as the type and amount of data involved, the sensitivity and context of the data, the likelihood and severity of harm, the characteristics of the recipients or unauthorized parties who accessed the data, and the mitigating measures taken or available to reduce the harm7Based on this analysis, the privacy officer can then decide whether to notify the affected individuals, the relevant authorities, or other stakeholders about the breach or incident.Notification is usually required by law or best practice when there is a high risk of harm to the individuals as a result of the breach or incident8Notification can also help to mitigate the harm by allowing the individuals to take protective actions or seek remedies.Therefore, performing a risk of harm analysis is a crucial first step for responding to a data breach or incident.Reference:5:Can a risk of harm itself be a harm? | Analysis | Oxford Academic;6:No Harm Done? Assessing Risk of Harm under the Federal Breach Notification Rule;7:CCOHS: Hazard and Risk - Risk Assessment;8: Breach Notification Requirements in Canada | PrivacySense.net

QUESTION 50
SCENARIO
Please use the following to answer the next QUESTION:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production -- not data processing -- and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.
To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth -- his uncle's vice president and longtime confidante -- wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.
Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.
After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.
Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.
Documentation of this analysis will show auditors due diligence.
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.
To improve the facility's system of data security, Anton should consider following through with the plan for which of the following?

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

Correct Answer: D
Section:
Explanation:
To improve the facility's system of data security, Anton should consider following through with the plan for controlled access at the company headquarters. This plan would help to prevent unauthorized physical access to the paper files, disks, and old computers that contain personal data of employees and customers.Physical security is an important aspect of data security that involves protecting hardware and storage devices from theft, damage, or tampering1By placing restrictions on who can enter the premises or access certain areas or rooms, Anton can reduce the risk of data breaches or incidents caused by intruders or insiders2He can also implement locks, alarms, cameras, or guards to enhance the physical security of the facility3Reference:1:Physical Security: What Is It?;2: [Physical Security: Why It's Important & How To Implement It];3: [Physical Security Best Practices: 10 Tips to Secure Your Workplace]

QUESTION 51
SCENARIO
Please use the following to answer the next QUESTION:
Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production -- not data processing -- and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.
To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth -- his uncle's vice president and longtime confidante -- wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.
Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.
After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.
Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.
Documentation of this analysis will show auditors due diligence.
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.

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

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

Correct Answer: C
Section:
Explanation:
Anton's objective for zero loss of personal information is the most unachievable among his plans for improving the data management of the company. While this objective is admirable and desirable, it is unrealistic and impractical to guarantee that no personal information will ever be lost due to a data breach or incident.Data breaches are inevitable and unpredictable events that can affect any organization regardless of its size or industry4Even with the best data security practices and tools in place, there is always a possibility of human error, system failure, malicious attack, or natural disaster that could compromise personal information5Therefore, Anton should focus on minimizing the likelihood and impact of data breaches rather than aiming for zero loss of personal information.He should also prepare a data breach response plan that outlines how to detect, contain, assess, report, and recover from a data breach in a timely and effective manner6Reference:4: [Data Breaches Are Inevitable: Here's How to Protect Your Business];5: The Top 5 Causes Of Data Breaches;6: Data Breach Response: A Guide for Business - Federal Trade Commission

QUESTION 52
SCENARIO
Please use the following to answer the next QUESTION:
Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production -- not data processing -- and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.
To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth -- his uncle's vice president and longtime confidante -- wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.
Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.
After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.
Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.
Documentation of this analysis will show auditors due diligence.
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.
Which important principle of Data Lifecycle Management (DLM) will most likely be compromised if Anton executes his plan to limit data access to himself and Kenneth?

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

Correct Answer: A
Section:
Explanation:
The important principle of Data Lifecycle Management (DLM) that will most likely be compromised if Anton executes his plan to limit data access to himself and Kenneth is ensuring data retrievability.Data retrievability refers to the ability to access and use data when needed for business purposes or legal obligations1It involves maintaining the availability, integrity, and usability of data throughout its lifecycle2However, if Anton restricts data access to only himself and Kenneth, he will create a single point of failure and a bottleneck for data retrieval. This could pose several risks and challenges for the company, such as:
Losing data if Anton or Kenneth forgets the password or leaves the company without sharing it with others.

Delaying data retrieval if Anton or Kenneth is unavailable or unresponsive when someone else needs the data urgently.
Violating data protection laws or regulations that require data access by certain parties or authorities under certain circumstances.
Reducing data quality or accuracy if Anton or Kenneth fails to update or maintain the data properly.
Missing business opportunities or insights if Anton or Kenneth does not share the data with other relevant stakeholders or departments.
Therefore, Anton should reconsider his plan and adopt a more balanced and secure approach to data access management that follows the principle of least privilege.This means granting data access only to those who need it for their specific roles and responsibilities and revoking it when no longer needed3He should also implement proper authentication, authorization, encryption, backup, and audit mechanisms to protect the data from unauthorized or unlawful access, use, disclosure, alteration, or destruction4Reference:1:Data Retrievability: What Is It?;2:Data Lifecycle Management | IBM;3:What is Least Privilege? Definition & Examples;4:Technical Security Controls: Encryption, Firewalls & More

QUESTION 53
SCENARIO
Please use the following to answer the next QUESTION:
Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production -- not data processing -- and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.
To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth -- his uncle's vice president and longtime confidante -- wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.
Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.
After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.
Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.
Documentation of this analysis will show auditors due diligence.
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.
In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding?

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

Correct Answer: A
Section:
Explanation:
In terms of compliance with regulatory and legislative changes, Anton has a misconception regarding the timeline for monitoring. He believes that the company should be safe for another five years after conducting a compliance assessment and documenting the analysis. However, this is a risky and unrealistic assumption that could expose the company to legal liabilities and penalties. Regulatory and legislative changes are dynamic and frequent in today's business environment.They can affect various aspects of the company's operations, such as data protection, online marketing, consumer rights, labor laws, tax laws, environmental laws, etc5Therefore, the company needs to monitor these changes continuously and proactively to ensure compliance at all times. Waiting for five years to check for compliance again could result in missing important updates or requirements that could impact the company's business practices or obligations.Moreover, compliance monitoring is not only a one-time activity but an ongoing process that involves evaluating the effectiveness of the company's policies and procedures in meeting the regulatory standards and expectations6Compliance monitoring also helps to identify any gaps or weaknesses in the company's compliance program and take corrective actions to improve it.Therefore, Anton should revise his timeline for monitoring regulatory and legislative changes and adopt a more regular and systematic approach that aligns with the company's risk profile and regulatory environment.Reference:5: Regulatory Change Management: How To Keep Up With Regulatory Changes;6: Compliance Monitoring - What Is It?

QUESTION 54
SCENARIO
Please use the following to answer the next QUESTION:

Henry Home Furnishings has built high-end furniture for nearly forty years. However, the new owner, Anton, has found some degree of disorganization after touring the company headquarters. His uncle Henry had always focused on production -- not data processing -- and Anton is concerned. In several storage rooms, he has found paper files, disks, and old computers that appear to contain the personal data of current and former employees and customers. Anton knows that a single break-in could irrevocably damage the company's relationship with its loyal customers. He intends to set a goal of guaranteed zero loss of personal information.
To this end, Anton originally planned to place restrictions on who was admitted to the physical premises of the company. However, Kenneth -- his uncle's vice president and longtime confidante -- wants to hold off on Anton's idea in favor of converting any paper records held at the company to electronic storage. Kenneth believes this process would only take one or two years. Anton likes this idea; he envisions a password- protected system that only he and Kenneth can access.
Anton also plans to divest the company of most of its subsidiaries. Not only will this make his job easier, but it will simplify the management of the stored data. The heads of subsidiaries like the art gallery and kitchenware store down the street will be responsible for their own information management. Then, any unneeded subsidiary data still in Anton's possession can be destroyed within the next few years.
After learning of a recent security incident, Anton realizes that another crucial step will be notifying customers. Kenneth insists that two lost hard drives in Question are not cause for concern; all of the data was encrypted and not sensitive in nature. Anton does not want to take any chances, however. He intends on sending notice letters to all employees and customers to be safe.
Anton must also check for compliance with all legislative, regulatory, and market requirements related to privacy protection. Kenneth oversaw the development of the company's online presence about ten years ago, but Anton is not confident about his understanding of recent online marketing laws. Anton is assigning another trusted employee with a law background the task of the compliance assessment. After a thorough analysis, Anton knows the company should be safe for another five years, at which time he can order another check.
Documentation of this analysis will show auditors due diligence.
Anton has started down a long road toward improved management of the company, but he knows the effort is worth it. Anton wants his uncle's legacy to continue for many years to come.
What would the company's legal team most likely recommend to Anton regarding his planned communication with customers?

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

Correct Answer: D
Section:
Explanation:
The company's legal team would most likely recommend Anton to consider under what circumstances communication with customers is necessary after learning of a recent security incident. Communication with customers is an important aspect of data breach response as it can help to mitigate the harm caused by the breach, restore trust and confidence in the company, and comply with legal obligations or best practices.However, communication with customers is not always mandatory or advisable depending on the nature and severity of the breach and the potential impact on the customers7Therefore, Anton should consult with his legal team and evaluate the following factors before deciding whether to communicate with customers or not:
The type and amount of data involved in the breach and whether it includes personal or sensitive information that could expose the customers to identity theft, fraud, or other harms.
The likelihood and extent of harm that the customers could suffer as a result of the breach and whether they could take any actions to prevent or reduce it.
The legal or contractual obligations that the company has to notify the customers or the relevant authorities about the breach and the applicable laws or regulations that govern the notification process, such as the timing, content, and method of notification.
The potential benefits and risks of communicating with customers, such as enhancing transparency and accountability, providing assistance and remedies, or triggering negative reactions, reputational damage, or legal claims.
Based on these factors, Anton should determine whether communication with customers is necessary and appropriate in his case. If he decides to communicate with customers, he should follow some best practices, such as:
Communicating as soon as possible after discovering and containing the breach and having sufficient information to share.
Communicating clearly, honestly, and empathetically about what happened, what data was affected, what actions the company has taken or will take, and what steps the customers can or should take.
Communicating through multiple channels, such as email, phone, letter, website, or social media, depending on the preferences and expectations of the customers.
Communicating consistently and regularly with updates or follow-ups until the breach is resolved and the customers are satisfied8

QUESTION 55
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.

Correct Answer: C

Section:
Explanation:
The nongovernmental privacy organizations, Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC), were established to protect civil liberties and raise consumer awareness in the digital age.Both organizations are public interest research centers that focus on emerging privacy and civil liberties issues and advocate for the protection of privacy, freedom of expression, and democratic values in the information age12They conduct policy research, public education, litigation, publications, and advocacy to promote privacy rights and challenge threats to privacy from governments, corporations, or other actors12They also monitor and participate in the development of laws, regulations, standards, and technologies that affect privacy and civil liberties12Reference:1:About EPIC;2:About EFF

QUESTION 56
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.

Correct Answer: A
Section:
Explanation:
The main function of the Asia-Pacific Economic Cooperation Privacy Framework is enabling regional data transfers while protecting information privacy across APEC member economies.The Framework promotes a flexible approach to information privacy protection that avoids the creation of unnecessary barriers to information flows3It is based on a set of common privacy principles that are consistent with the core values of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data3The Framework also provides guidance for domestic implementation and international implementation of the privacy principles through various mechanisms, such as cross-border privacy rules (CBPRs), accountability agents, regulators, enforcement cooperation, and capacity building3The Framework aims to facilitate the safe transfer of information between economies, enhance consumer trust and confidence in online transactions and information networks, encourage the use of electronic data to enhance and expand business opportunities, and provide technical assistance to economies that have yet to address privacy from a regulatory or policy perspective4Reference:3:APEC PRIVACY PRINCIPLES;4:APEC Data Privacy Pathfinder

QUESTION 57
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.

Correct Answer: C
Section:
Explanation:
The statement that is true about the Data Protection Impact Assessment (DPIA) process as required under the General Data Protection Regulation (GDPR) is that the DPIA must include a description of the proposed processing operation and its purpose. According to Article 35(7) of the GDPR, a DPIA shall contain at least:
''a systematic description of the envisaged processing operations and the purposes of the processing'';
''an assessment of the necessity and proportionality of the processing operations in relation to the purposes'';
''an assessment of the risks to the rights and freedoms of data subjects'';
''the measures envisaged to address the risks'';
''safeguards'', ''security measures'';
''mechanisms to ensure the protection of personal data'';
''to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned''5
Therefore, a DPIA must include a description of what data processing activities are planned and why they are needed as part of its content.This helps to provide a clear overview of the processing operation and its objectives as well as to assess its necessity and proportionality in relation to its purposes6Reference:5: [General Data Protection Regulation (GDPR) -- Official Legal Text], Article 35(7);6: Data protection impact assessments | ICO

QUESTION 58

SCENARIO
Please use the following to answer the next QUESTION:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that ''appropriate'' data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations.
''We want Medialite to have absolutely the highest standards,'' he says. ''In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective.''
You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
The CEO likes what he's seen of the company's improved privacy program, but wants additional assurance that it is fully compliant with industry standards and reflects emerging best practices. What would best help accomplish this goal?

A. An external audit conducted by a panel of industry experts
B. An internal audit team accountable to upper management
C. Creation of a self-certification framework based on company policies
D. Revision of the strategic plan to provide a system of technical controls

Correct Answer: A
Section:
Explanation:
This approach provides an independent, unbiased review of the company's privacy program. External experts can assess the company's processes and controls against industry standards, benchmarks, and emerging best practices. This will not only provide the desired assurance but also potentially enhance the company's credibility in the eyes of stakeholders, as it shows a willingness to be transparent and undergo external scrutiny.

QUESTION 59
SCENARIO
Please use the following to answer the next QUESTION:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that ''appropriate'' data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations.
''We want Medialite to have absolutely the highest standards,'' he says. ''In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective.''
You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
The 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

Correct Answer: D

Section:
Explanation:
Shifting attention to privacy for emerging technologies as the company begins to use them is a logical next step to help ensure a high level of protection. Emerging technologies, such as artificial intelligence, biometrics, blockchain, cloud computing, internet of things, etc., may pose new challenges and opportunities for privacy and data protection. They may involve new types, sources, uses, and flows of personal data that require different or additional safeguards and controls. They may also introduce new risks or impacts for individuals' rights and interests that require careful assessment and mitigation. Therefore, it is important for the company to consider and address the privacy implications of emerging technologies as they adopt or integrate them into their products, services, or processes.
The other options are not as logical or effective as shifting attention to privacy for emerging technologies for ensuring a high level of protection. Brainstorming methods for developing an enhanced privacy framework may not be necessary or feasible if the company already has established new best practices for the industry. Developing a strong marketing strategy to communicate the company's privacy practices may not be sufficient or relevant for ensuring a high level of protection, as it may not reflect the actual state or quality of the privacy program. Focusing on improving the incident response plan in preparation for any breaks in protection may be too reactive or narrow in scope, as it may not cover other aspects or dimensions of privacy and data protection that require continuous monitoring and improvement.
For more information on privacy for emerging technologies, you can refer to these sources:
[Privacy by Design in Emerging Technologies]
[Privacy Challenges in Emerging Technologies]
[Privacy Enhancing Technologies]

QUESTION 60
SCENARIO
Please use the following to answer the next QUESTION:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that ''appropriate'' data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. ''We want Medialite to have absolutely the highest standards,'' he says. ''In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective.''
You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
What metric can Goddard use to assess whether costs associated with implementing new privacy protections are justified?

A. Compliance ratio
B. Cost-effective mean
C. Return on investment
D. Implementation measure

Correct Answer: C
Section:
Explanation:
This answer is the best metric that Goddard can use to assess whether the costs associated with implementing new privacy protections are justified, as it can measure the financial benefits or value that the privacy protections generate for the company in relation to the costs or expenses that they incur. Return on investment (ROI) is a ratio that compares the net income or profit from an investment to the initial or total cost of the investment. ROI can help to evaluate the efficiency and effectiveness of an investment, as well as to compare different investments or alternatives. ROI can also help to support decision making and budget allocation for privacy protection initiatives.

QUESTION 61
SCENARIO
Please use the following to answer the next QUESTION:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically Questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the

target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that ''appropriate'' data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures.
He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. ''We want Medialite to have absolutely the highest standards,'' he says. ''In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective.''
You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
You 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.

Correct Answer: B
Section:
Explanation:
This answer is the best way to describe what it means to have a ''managed'' privacy program, according to the AICPA/CICA Privacy Maturity Model (PMM), which is a framework that measures the effectiveness and maturity of an organization's privacy program based on five phases: ad hoc, repeatable, defined, managed and optimized. The managed phase is the fourth level of maturity in the PMM, which indicates that the organization has a formal and consistent approach to privacy protection and that its privacy practices are aligned with its policies and objectives. The managed phase means that the organization has procedures and processes that are fully documented and implemented, and cover all relevant aspects of data collection, use, storage, protection, sharing and disposal. The managed phase also means that the organization has controls and measures that are monitored and evaluated regularly, and that any issues or incidents are reported and resolved promptly.

QUESTION 62
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.

Correct Answer: D
Section:
Explanation:
As a Data Protection Officer (DPO), one of the most effective ways to execute your responsibility of monitoring changes in laws and regulations and updating policies accordingly is to subscribe to email list-serves that report on regulatory changes.Email list-serves are online mailing lists that allow subscribers to receive regular updates on topics or issues of interest via email7By subscribing to email list-serves that report on regulatory changes, you can stay informed of the latest developments and trends in the regulatory environment that affect your organization and its data protection practices.You can also access relevant information and resources from reliable sources, such as regulatory agencies, law firms, industry associations, or experts8This can help you to identify and analyze the impact of regulatory changes on your organization and its data processing activities, and to update your policies and procedures accordingly to ensure compliance8Some examples of email list-serves that report on regulatory changes are:
The ICO Newsletter: This is a monthly newsletter from the UK Information Commissioner's Office (ICO) that provides updates on data protection news, guidance, events, consultations, and enforcement actions9
The Privacy Advisor: This is a monthly newsletter from the International Association of Privacy Professionals (IAPP) that covers global privacy news, analysis, and insights10
The Privacy & Data Security Law Journal: This is a monthly journal from LexisNexis that provides articles and case notes on privacy and data security law issues from around the world11
The Data Protection Report: This is a blog from Norton Rose Fulbright that provides updates and commentary on data protection and cybersecurity developments across various jurisdictions12

QUESTION 63

SCENARIO
Please use the following to answer the next QUESTION:
John is the new privacy officer at the prestigious international law firm -- A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.
During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor -- MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.
John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.
At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.
Which of the following is the most effective control to enforce MessageSafe's implementation of appropriate technical countermeasures to protect the personal data received from A&M LLP?

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

Correct Answer: C
Section:
Explanation:
The most effective control to enforce MessageSafe's implementation of appropriate technical countermeasures to protect the personal data received from A&M LLP is to require MessageSafe to apply appropriate security controls on the cloud infrastructure. This control ensures that MessageSafe takes responsibility for securing the personal data that it processes on behalf of A&M LLP on the cloud platform provided by Cloud Inc.According to the GDPR, data processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing personal data1These measures may include encryption, pseudonymisation, access control, backup and recovery, logging and monitoring, vulnerability management, incident response, etc2Furthermore, data processors must ensure that any sub-processors they engage to process personal data on behalf of the data controller also comply with the same obligations3Therefore, MessageSafe must ensure that Cloud Inc. provides adequate security guarantees for the cloud infrastructure and services that it uses to host the email continuity service for A&M LLP. MessageSafe must also monitor and audit the security performance of Cloud Inc.and report any issues or breaches to A&M LLP.Reference:1:Article 32 GDPR | General Data Protection Regulation (GDPR);2:Guidelines 4/2019 on Article 25 Data Protection by Design and by Default | European Data Protection Board;3:Article 28 GDPR | General Data Protection Regulation (GDPR)

QUESTION 64
SCENARIO
Please use the following to answer the next QUESTION:
John is the new privacy officer at the prestigious international law firm -- A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.
During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor -- MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.
John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.
At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off- premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.
Which of the following is a TRUE statement about the relationship among the organizations?

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

Correct Answer: B
Section:
Explanation:
A true statement about the relationship among the organizations is that MessageSafe is liable if Cloud Inc. fails to protect data from A&M LLP.This statement reflects the principle of accountability under the GDPR, which requires data controllers and processors to be responsible for complying with the GDPR and demonstrating their compliance4As a data processor for A&M LLP, MessageSafe is liable for any damage caused by processing that infringes the GDPR or by processing that does not comply with A&M LLP's lawful instructions5This liability extends to any sub-processors that MessageSafe engages to carry out specific processing activities on behalf of A&M LLP5Therefore, if Cloud Inc., as a sub-processor for MessageSafe, fails to protect data from A&M LLP and causes harm to the data subjects or breaches the GDPR or A&M LLP's instructions, MessageSafe will be held liable for such failure and may have to pay compensation or face administrative fines or other sanctions6Reference:4:Article 5 GDPR | General Data Protection Regulation (GDPR);5:Article 82 GDPR | General Data Protection Regulation (GDPR);6:Article 83 GDPR | General Data Protection Regulation (GDPR)

QUESTION 65
SCENARIO
Please use the following to answer the next QUESTION:
John is the new privacy officer at the prestigious international law firm -- A&M LLP. A&M LLP is very proud of its reputation in the practice areas of Trusts & Estates and Merger & Acquisition in both U.S. and Europe.
During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm's email continuity service to their existing email security vendor -- MessageSafe. Being successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for A&M LLP.
John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe's previous breach and learned that the breach was caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.
At the meeting, Derrick emphasized that email is the primary method for the firm's lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn't have the time or resource to look for another solution. Furthermore, the off- premises email continuity service will only be turned on when the email service at A&M LLP's primary and secondary data centers are both down, and the email messages stored at MessageSafe site for continuity service will be automatically deleted after 30 days.
Which of the following is NOT an obligation of MessageSafe as the email continuity service provider for A&M LLP?

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

Correct Answer: C
Section:
Explanation:
An obligation that is not applicable to MessageSafe as the email continuity service provider for A&M LLP is obtaining certifications to relevant frameworks.Certifications are voluntary mechanisms that enable data controllers or processors to demonstrate their compliance with the GDPR or other standards by obtaining a certification issued by an accredited certification body7Certifications can provide benefits such as enhancing transparency, accountability, trust, and competitive advantage for data controllers or processors.However, they are not mandatory under the GDPR or other laws and do not reduce or eliminate the legal obligations or liabilities of data controllers or processors8Therefore, MessageSafe is not obliged to obtain certifications to relevant frameworks as the email continuity service provider for A&M LLP.However, it may choose to do so if it wishes to showcase its compliance efforts or gain a competitive edge in the market.Reference:7:Article 42 GDPR | General Data Protection Regulation (GDPR);8:Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679 | European Data Protection Board

QUESTION 66
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.

Correct Answer: B

Section:
Explanation:
A covered entity is an organization that is subject to the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA regulates how covered entities use and disclose protected health information (PHI) of individuals. Covered entities include health plans, health care clearinghouses, and health care providers that transmit health information electronically.Reference: [HIPAA for Professionals], [What is a Covered Entity?]

QUESTION 67
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.

Correct Answer: B
Section:
Explanation:
The first major goal of a company developing a new privacy program should be to schedule conversations with executives of affected departments. This is because a privacy program requires the support and involvement of senior management and key stakeholders from different business units, such as legal, IT, marketing, human resources, etc. By engaging with them early on, a privacy professional can understand their needs, expectations, challenges, and risks, and align the privacy program objectives and strategies with the organization's goals and culture.Reference: [How to Develop a Privacy Program], [Privacy Program Management]

QUESTION 68
''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

Correct Answer: C
Section:
Explanation:
The metric life cycle is a process that involves collecting, accessing, analyzing, reporting, and destroying data. These aspects are essential for measuring the performance and effectiveness of privacy programs.Reference:IAPP CIPM Study Guide, page 14.

QUESTION 69
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

Correct Answer: B
Section:
Explanation:
To rationalize data protection requirements means to look for overlaps in laws and regulations from which a common solution can be developed. This can help simplify compliance efforts and reduce costs and complexity.Reference:IAPP CIPM Study Guide, page 16.

QUESTION 70
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

Correct Answer: D
Section:
Explanation:
A single attribute is a term that describes a piece of personal data that alone may not identify an individual, such as a first name or a zip code. However, when combined with other attributes, it may become identifiable.Reference:IAPP CIPM Study Guide, page 18.

QUESTION 71
SCENARIO
Please use the following to answer the next QUESTION:
Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.
Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the ''misunderstanding'' has not occurred again.
As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.
Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. ''The good news,'' he says, ''is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud.''
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.

Correct Answer: B
Section:
Explanation:
This answer is the primary data protection issue with cloud computing that Albert should be concerned about, as it can affect the confidentiality, integrity and availability of the data that is stored and processed on the cloud. Outdated security frameworks refer to the lack of or insufficient technical and organizational measures that are implemented by the cloud service provider or the cloud user to protect the data from unauthorized or unlawful access, use, disclosure, alteration or destruction. Outdated security frameworks can include weak encryption, authentication, authorization, logging, monitoring, backup or recovery mechanisms, as well as inadequate policies, procedures, standards or best practices for data security. Outdated security frameworks can expose the data to various threats and risks, such as cyberattacks, data breaches, data loss or corruption, or legal actions.

QUESTION 72
SCENARIO
Please use the following to answer the next QUESTION:
Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced

options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.
Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the ''misunderstanding'' has not occurred again.
As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.
Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. ''The good news,'' he says, ''is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud.''
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

Correct Answer: C
Section:
Explanation:
This answer is the best way to prevent the Finnish vendor from transferring data to another party, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for data processing activities. Including transfer prohibitions in the vendor contract can help to define the scope, purpose, duration and type of data processing, as well as the rights and obligations of both parties. The contract can also specify that the vendor is not allowed to share, disclose or transfer the data to any third party without the prior consent or authorization of the organization, and that any breach of this clause may result in legal actions, penalties or termination of the contract.

QUESTION 73
SCENARIO
Please use the following to answer the next QUESTION:
Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.
Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the ''misunderstanding'' has not occurred again.
As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.
Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. ''The good news,'' he says, ''is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud.''
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

Correct Answer: A
Section:
Explanation:
This answer is the best process to answer Albert's questions about the vendor's data security safeguards, as it can provide a direct and comprehensive way to assess and verify the vendor's compliance with the applicable laws, regulations, standards and best practices for data protection. A second-party or supplier audit is conducted by the organization that hires or contracts the vendor to evaluate their performance and alignment with the organization's standards and expectations. A second-party or supplier audit can also help to identify any gaps, weaknesses or risks in the vendor's data security safeguards, and to recommend or require any improvements or corrective actions.

QUESTION 74
SCENARIO
Please use the following to answer the next QUESTION:
As they company's new chief executive officer, Thomas Goddard wants to be known as a leader in data protection. Goddard recently served as the chief financial officer of Hoopy.com, a pioneer in online video viewing with millions of users around the world. Unfortunately, Hoopy is infamous within privacy protection circles for its ethically questionable practices, including unauthorized sales of personal data to marketers. Hoopy also was the target of credit card data theft that made headlines around the world, as at least two million credit card numbers were thought to have been pilfered despite the company's claims that ''appropriate'' data protection safeguards were in place. The scandal affected the company's business as competitors were quick to market an increased level of protection while offering similar entertainment and media content. Within three weeks after the scandal broke, Hoopy founder and CEO Maxwell Martin, Goddard's mentor, was forced to step down.
Goddard, however, seems to have landed on his feet, securing the CEO position at your company, Medialite, which is just emerging from its start-up phase. He sold the company's board and investors on his vision of Medialite building its brand partly on the basis of industry-leading data protection standards and procedures. He may have been a key part of a lapsed or even rogue organization in matters of privacy but now he claims to be reformed and a true believer in privacy protection. In his first week on the job, he calls you into his office and explains that your primary work responsibility is to bring his vision for privacy to life. But you also detect some reservations. ''We want Medialite to have absolutely the highest standards,'' he says. ''In fact, I want us to be able to say that we are the clear industry leader in privacy and data protection. However, I also need to be a responsible steward of the company's finances. So, while I want the best solutions across the board, they also need to be cost effective.''
You are told to report back in a week's time with your recommendations. Charged with this ambiguous mission, you depart the executive suite, already considering your next steps.
You are charged with making sure that privacy safeguards are in place for new products and initiatives. What is the best way to do this?

A. Hold a meeting with stakeholders to create an interdepartmental protocol for new initiatives
B. Institute Privacy by Design principles and practices across the organization
C. Develop a plan for introducing privacy protections into the product development stage
D. Conduct a gap analysis after deployment of new products, then mend any gaps that are revealed

Correct Answer: B
Section:
Explanation:
Privacy by Design principles ensure that privacy considerations are integrated from the very beginning and throughout the entire product or initiative development process. This proactive approach not only ensures that privacy safeguards are in place from the start but can also be more cost-effective in the long run as it helps prevent potential breaches or issues that might arise later, saving on potential fines, reputational damage, and corrective actions.

QUESTION 75
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

Correct Answer: D
Section:
Explanation:
The decrease of mean time to resolve privacy incidents best demonstrates the effectiveness of a firm's privacy incident response process. This metric measures how quickly and efficiently the firm can identify, contain, analyze, remediate, and report privacy incidents. A lower mean time to resolve indicates a higher level of preparedness, responsiveness, and resilience in handling privacy incidents.Reference:IAPP CIPM Study Guide, page 25.

QUESTION 76
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

Correct Answer: D
Section:
Explanation:
The results from a previous information audit can be leveraged in a PIA process. An information audit is a systematic review of the personal data that an organization holds, such as its sources, purposes, locations, flows, and retention periods. An information audit can provide valuable input for a PIA, as it can help identify the types and categories of personal data that will be involved in the project, as well as the potential risks and impacts associated with them.Reference:IAPP CIPM Study Guide, page 27.

QUESTION 77
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseo is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseo 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 Briseo 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 Briseo'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. Briseo 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

Correct Answer: B

Section:

QUESTION 78
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseo is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseo 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 Briseo 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 Briseo'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. Briseo 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

Correct Answer: B
Section:

QUESTION 79
SCENARIO
Please use the following to answer the next QUESTION:
Martin Briseo is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseo 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 Briseo 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 Briseo'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. Briseo 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

Correct Answer: D
Section:

QUESTION 80
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

Correct Answer: D
Section:
Explanation:
A personal information inventory is a document that assists the Privacy Manager in identifying and responding to a request from an individual about what personal information the organization holds about them and with whom the information is shared. A personal information inventory is a comprehensive and detailed record of all personal information that an organization collects, uses, discloses, stores, and disposes of. It helps an organization map its data flows, assess its privacy risks, comply with its legal obligations, and respond to data subject requests. A personal information inventory should include information such as: the categories and sources of personal information; the purposes and legal bases for processing; the recipients and transfers of personal information; the retention periods and disposal methods; and the security measures and safeguards.
CIPM Body of Knowledge (2021), Domain IV: Privacy Program Operational Life Cycle, Section B: Protecting Personal Information, Subsection 3: Data Inventory
CIPM Study Guide (2021), Chapter 8: Protecting Personal Information, Section 8.3: Data Inventory
CIPM Textbook (2019), Chapter 8: Protecting Personal Information, Section 8.3: Data Inventory
CIPM Practice Exam (2021), Question 138

QUESTION 81
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.

Correct Answer: A
Section:
Explanation:
The optimum first step to take when creating a Privacy Officer governance model is to involve senior leadership. Senior leadership plays a crucial role in establishing and supporting a privacy program within an organization. They can provide strategic direction, allocate resources, approve policies, endorse initiatives, communicate values, and demonstrate accountability. By involving senior leadership from the beginning, a Privacy Officer can ensure that the privacy program aligns with the organization's vision, mission, goals, and culture. Senior leadership can also help overcome potential barriers or resistance from other stakeholders by endorsing and promoting the privacy program.
CIPM Body of Knowledge (2021), Domain I: Privacy Program Governance, Section A: Privacy Governance Models, Subsection 1: Privacy Officer Governance Model
CIPM Study Guide (2021), Chapter 2: Privacy Governance Models, Section 2.1: Privacy Officer Governance Model
CIPM Textbook (2019), Chapter 2: Privacy Governance Models, Section 2.1: Privacy Officer Governance Model
CIPM Practice Exam (2021), Question 139

QUESTION 82
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.

Correct Answer: D
Section:
Explanation:
Providing a dedicated privacy space with the privacy policy, explanatory documents and operation frameworks helps build trust with customers and stakeholders. A dedicated privacy space is a section on an organization's website or app that provides clear and transparent information about how the organization processes personal information and respects data subject rights. It can include documents such as: a privacy policy that explains what personal information is collected, why it is collected, how it is used, who it is shared with, and how it is protected; explanatory documents that provide more details or examples of specific processing activities or scenarios; and operation frameworks that describe the procedures and mechanisms for data subject requests, complaints, inquiries, or feedback. A dedicated privacy space can help customers and stakeholders understand the organization's privacy practices, choices, and values, and enhance their confidence and trust.
CIPM Body of Knowledge (2021), Domain II: Privacy Program Framework, Section A: Privacy Program Framework Components, Subsection 1: Privacy Policies
CIPM Study Guide (2021), Chapter 4: Privacy Program Framework Components, Section 4.1: Privacy Policies
CIPM Textbook (2019), Chapter 4: Privacy Program Framework Components, Section 4.1: Privacy Policies
CIPM Practice Exam (2021), Question 140

QUESTION 83
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

Correct Answer: C
Section:

Explanation:
Organizational culture is not an important factor to consider when developing a data retention policy. A data retention policy is a document that defines how long an organization retains personal information for various purposes and how it disposes of it securely when it is no longer needed. A data retention policy should be based on factors such as: business requirements, such as operational needs, customer expectations, contractual obligations, or industry standards; compliance requirements, such as legal obligations, regulatory mandates, or audit recommendations; and technology resources, such as storage capacity, backup systems, encryption methods, or disposal tools. Organizational culture, which refers to the values, beliefs, norms, and behaviors that shape how an organization operates and interacts with its stakeholders, is not a relevant factor for determining data retention periods or disposal methods.
CIPM Body of Knowledge (2021), Domain IV: Privacy Program Operational Life Cycle, Section B: Protecting Personal Information, Subsection 4: Data Retention
CIPM Study Guide (2021), Chapter 8: Protecting Personal Information, Section 8.4: Data Retention
CIPM Textbook (2019), Chapter 8: Protecting Personal Information, Section 8.4: Data Retention
CIPM Practice Exam (2021), Question 141

QUESTION 84
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.

Correct Answer: B
Section:
Explanation:
When expanding into a new jurisdiction, it is not necessary to appoint a new Privacy Officer (PO) for that jurisdiction, unless the local law requires it. The other options are important steps to ensure compliance with the new jurisdiction's privacy laws and regulations, as well as to align the privacy program with the business objectives and culture of the new market.Reference:CIPM Body of Knowledge, Domain I: Privacy Program Governance, Task 1: Establish the privacy program vision and strategy.

QUESTION 85
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.

Correct Answer: C
Section:
Explanation:
A data inventory is a good starting point to understand the scope of privacy program needs, as it provides a comprehensive overview of what personal data is collected, processed, stored, shared, and disposed of by the organization. A data inventory can help identify the legal obligations, risks, and gaps in the privacy program, as well as the opportunities for improvement and optimization. The other options are also important components of a privacy program, but they are more effective when based on a data inventory.Reference:CIPM Body of Knowledge, Domain II: Privacy Program Operational Life Cycle, Task 1: Assess the current state of the privacy program.

QUESTION 86
What is the name for the privacy strategy model that describes delegated decision making?

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

D. Matrix.

Correct Answer: D
Section:
Explanation:
A matrix is a type of organizational structure that involves delegated decision making. In a matrix structure, employees report to more than one manager or leader, usually based on different functions or projects. For example, a software developer may report to both a product manager and a technical manager. A matrix structure allows for more flexibility, collaboration, and innovation in complex and dynamic environments.
The other options are not examples of delegated decision making structures. A de-centralized structure involves distributing decision making authority across different levels or units of the organization, rather than concentrating it at the top. A de-functionalized structure involves breaking down functional silos and creating cross-functional teams or processes. A hybrid structure involves combining elements of different types of structures, such as functional, divisional, or matrix.

QUESTION 87
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.

Correct Answer: A
Section:
Explanation:
The PCI DSS framework does not require implementing strong asset control protocols. Asset control protocols are policies and procedures that govern how an organization manages its physical and digital assets, such as inventory, equipment, software, data, etc. Asset control protocols may include aspects such as identification, classification, valuation, tracking, maintenance, disposal, etc. Asset control protocols are important for ensuring the security and integrity of an organization's assets, but they are not part of the PCI DSS framework.

QUESTION 88
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.

Correct Answer: A
Section:
Explanation:
Binding Corporate Rules (BCRs) are a set of legally binding rules that allow multinational corporations or groups of companies to transfer personal data across borders within their organization in compliance with the EU data protection law1BCRs are approved by the competent data protection authorities in the EU and are enforceable by data subjects and the authorities2BCRs are one of the mechanisms recognized by the EU General Data Protection Regulation (GDPR) to ensure an adequate level of protection for personal data transferred outside the European Economic Area (EEA)3

QUESTION 89
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.

Correct Answer: D
Section:
Explanation:
The marketing team needs a check box for their SMS opt-in because it is part of the consumer's right to be informed. This right means that consumers have the right to know how their personal data is collected, used, shared, and protected by the organization. The check box allows consumers to give their consent and opt-in to receive SMS messages from the organization, and also informs them of the purpose and scope of such messages. The other rights are not relevant in this case, as they are related to other aspects of data processing, such as correction, complaints, and access.Reference:CIPM Body of Knowledge, Domain IV: Privacy Program Communication, Section A: Communicating to Stakeholders, Subsection 1: Consumer Rights.

QUESTION 90
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.

Correct Answer: B
Section:
Explanation:
When conducting due diligence during an acquisition, a privacy professional should avoid allowing legal in both companies to handle the privacy laws and compliance. This is because legal teams may not have the expertise or the resources to address all the privacy issues and risks that may arise from the acquisition. A privacy professional should be involved in the due diligence process to ensure that the privacy policies, practices, and obligations of both companies are aligned and compliant with the applicable laws and regulations. The other options are not things that a privacy professional should avoid, but rather things that they should do as part of the due diligence process.Reference:CIPM Body of Knowledge, Domain V: Privacy Program Management, Section A: Privacy Program Administration, Subsection 3: Due Diligence.