Sample Exam

Edition 202301

Content

Introduction

This is the EXIN Privacy & Data Protection Professional (PDPP.EN) sample exam. The Rules and Regulations for EXIN's examinations apply to this exam.

This exam consists of 40 multiple-choice questions. Each multiple-choice question has a number of possible answers, of which only one is correct.

The maximum number of points that can be obtained for this exam is 40. Each correct answer is worth 1 point. You need 26 points or more to pass the exam.

The time allowed for this exam is 120 minutes.

You are allowed to use the GDPR text for this exam.

Good luck!

Sample Exam

1 / 40
A company implements a privacy policy, which helps to demonstrate compliance with the GDPR. It is recommended that this policy is made publicly accessible for several reasons.

What is the **main** reason for making the privacy policy publicly available?

A) To allow customers and partners to verify which personal data the organization must process
B) To allow customers, partners and the supervisory authority to assess how personal data are handled
C) To communicate the result of data protection impact assessments (DPIAs) performed in the organization
D) To inform the supervisory authority of how the organization will respond after personal data breaches

2 / 40
According to the GDPR, what information is **not** a mandatory part of a privacy policy?

A) Information about international transfers of personal data to a third country
B) Information about the identity and contact details of the controller
C) Information relating to data security measures in the organization
D) Information relating to retention periods and data subject's rights

3 / 40
The GDPR embraces the principles of privacy by design and by default. The application of these principles includes the implementation of both technical and organizational measures.

Why are organizational measures necessary?

A) Because privacy by design and by default requires that the organization restricts personal data access to controllers only
B) Because protecting the rights of data subjects, requires organizational processes that technical measures cannot cover
C) Because the designation of a data protection officer (DPO), where mandatory, is regarded as an organizational measure

4 / 40
A company is setting up a project to create a new, free service for consumers.

According to privacy by design, what is the **most** desirable time to discuss data protection?

A) From the start of the project
B) During the implementation phase
C) When the project nears completion

5 / 40
An organization is implementing the privacy information management system (PIMS) using the ISO/IEC 27701 standard.

During the implementation, some of the organization's contractors realize that they must comply with several legal requirements from different countries. The contractors decide to ask the data protection officer (DPO) for advice.

According to ISO/IEC 27701, how should the DPO categorize the legal requirements?

A) Internal issue because the legal requirements directly impact the PIMS, which is an internal matter.
B) Internal issue because the relevant factors are the contractors who must be seen as coworkers.
C) External issue because the contractors operate outside the regular coworkers of the organization.
D) External issue because the legal requirements are relevant but independent from the organization.

6 / 40
A business to consumer (B2C) organization is implementing a privacy information management system (PIMS).

The data protection officer (DPO) comes across the following media that contain information:

- An **external hard drive** with competitor information and a description of their strengths and weaknesses.
- Some **paper files** from human resources (HR) with health information and emergency contact information in them.
- A computer **server** which contains a backup of all customer data, including of direct consumers.
- Old **USB drives** with former coworkers' personal information and their last salaries at the organization.

Which media do **not** have to be part of the PIMS?

A) External hard drive
B) Paper files
C) Server
D) USB drives

7 / 40
When defining a privacy information management system (PIMS), different documents are created. One of these documents is the statement of applicability (SoA).

What is a statement of applicability (SoA)?

A) The SoA gauges how likely it is that processing data results in a high risk to individuals.
B) The SoA records where and how personal data of employees and customers is processed.
C) The SoA states which controls must be applied to manage or minimize risk within the PIMS.

8 / 40
It is fundamental to a privacy information management system (PIMS), both in the short and long term, to be able to demonstrate how corporate policies, operating procedures, and work instructions are formulated. This ensures that actions are traceable to management decisions and policies, and that the results are reproducible.

Which requirement of the PIMS is this referring to?

A) Audit
B) Documentation
C) Management review
D) Statement of applicability (SoA)

9 / 40
Why should top management review the progress of the privacy information management system (PIMS)?

A) To ensure that the PIMS conforms with all relevant legal requirements
B) To ensure that the PIMS has enough privacy controls to mitigate risks
C) To ensure that the PIMS is audited regularly and is producing documents
D) To ensure that the PIMS is effective and meets corporate requirements

10 / 40
Auditing the privacy information management system (PIMS) can be done for multiple reasons.

According to ISO/IEC 27701, what is the **main** objective of PIMS audits?

A) To confirm that requirements of the relevant national and international standards are maintained
B) To identify specific areas of concern and address the selection of individual work processes
C) To include updates of relevant changes to legislation and regulations, and their interpretation
D) To monitor conformity between the management system requirements and working practices

11 / 40
An organization implements a privacy information management system (PIMS). The specific requirements must be based on local rules and contractual requirements.

What should be the next step for the organization's legal team?

A) Hire local legal advice and guidance, and apply the ISO/IEC 27701 as the contractual standard to clients and suppliers
B) Look up the applicable international best practices, and review all contracts which involve personal data processing
C) Map the applicable legislation and related legal sanctions, and review all contracts which involve personal data processing
D) Request local supervisory authority's guidance, and apply the ISO/IEC 27701 as a contractual standard to clients and suppliers

12 / 40
An organization is merging with another company. The organization already has a privacy information management system (PIMS).

The completion of the process depends on demonstrating that all the personal data processing operations follow the ISO/IEC 27701 and the applicable legislation.

What is the **most** appropriate means to show this?

A) A data protection impact assessment (DPIA) report
B) A privacy impact assessment (PIA) report
C) A recent PIMS audit report
D) A statement of applicability (SoA) report

13 / 40
A small organization has developed a successful software service. Their service is a large success, which means the organization needs a more robust cloud solution. Therefore, the organization must select an external cloud supplier.

The organization is ISO/IEC 27701 certified. When searching for a supplier, the organization comes across several cloud suppliers. Some suppliers are ISO/IEC 27701 certified, but others are not.

How can an ISO/IEC 27701 certification help with supplier selection?

A) The ISO/IEC 27701 certification of a supplier includes a cost/benefit analysis, which ensures lower costs for services.
B) The ISO/IEC 27701 certification of a supplier lowers the need for supplier audits, which is easier for the organization.
C) The ISO/IEC 27701 certification of the organization has procedures for data processing, which extends to any supplier.
D) The ISO/IEC 27701 certification of the organization requires an ISO/IEC 27701 certified supplier, which limits choices.

14 / 40
When working towards ISO/IEC 27701 certification, there are several management systems involved. Two of these systems are:

- the privacy information management system (PIMS)
- the information security management system (ISMS)

What is true about these systems?

A) The ISMS and PIMS audits may be combined or done separately, even though the PIMS requirements depend on the maintenance of the ISMS.
B) The ISMS and PIMS audits must never be done together, because the PIMS and ISMS system requirements do not depend on each other.
C) The ISMS is part of the PIMS and addresses information protection, since the ISMS looks at a business risk approach to personal data.

15 / 40
An organization is implementing a privacy information management system (PIMS). The GDPR requires that “personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data […]”.

What is the relationship between this requirement and the ISO/IEC 27701 standard?

A) The GDPR principles of integrity and confidentiality form the foundation of the PIMS that is required for the ISO/IEC 27701 standard.
B) The GDPR principles of lawfulness, fairness, and transparency contribute to the PIMS and the information security management system (ISMS).
C) The GDPR principle of purpose limitation prescribes exactly how the data that fall under the PIMS may or may not be used.
D) The GDPR principle of storage limitation explains the length of time the personal data reside in the PIMS before processing.

16 / 40
The ISO/IEC 27701 standard contains a chapter dedicated to additional guidance that aligns with the ISO/IEC 27002 standard.

What type of recommendations are **not** included in this chapter?

A) Develop privacy policies separate from or combined with information security policies
B) Ensure at least awareness training for all coworkers that handle or process personal data
C) Label all data clearly to identify where personal data is stored or otherwise processed
D) Plan internal and external audits with a specific interval depending on the audit scope

17 / 40
Applying privacy information management system (PIMS) controls to manage risk is not an easy task, and it is recommended to go through all the stages.

The first stage is to design a set of controls to manage risks. The other stages are listed below (in random order):

1. Compare controls to ISO/IEC 27701’s Annex A or B
2. Produce the statement of applicability (SoA)
3. Effectively implement the controls

What is the **correct** order of the other stages?

A) 1, 2, 3
B) 1, 3, 2
C) 2, 1, 3
D) 2, 3, 1

18 / 40
According to the GDPR, which activity is always a responsibility of the controller?

A) Being responsible for performing a data protection impact assessment (DPIA)
B) Contracting a security company for the protection of personal data in transit
C) Implementing a new method to collect personal data from the customers
D) Maintaining records of the processing activities carried out by the processor

19 / 40
A hospital outsources its printing of patient invoices to a printing company. The printing company also prints invoices for other organizations.

Due to an error, names and addresses were mixed up when they were sorted at the printing company, and a number of invoices were sent to the wrong patients.

The hospital had carefully analyzed their own processes. The hospital had a robust verification process in place and has contractual agreements with the printing company.

Why will the hospital be held **responsible** by the supervisory authority?

A) Because the contract determines this
B) Because the hospital is the controller
C) Because the mix-up is between patients
D) Because the verification has gone wrong

20 / 40
When a controller and a processor sign a contract for the processing of personal data, they both have specific responsibilities. Some of these responsibilities are prescribed by the GDPR and others can be arranged in the contract.

According to the GDPR, when does the processor always need written authorization by the controller?

A) When the processor contracts a company to protect data during transfers
B) When the processor contracts a third party to process personal data
C) When the processor implements a new method to collect personal data
D) When the processor implements a new method to delete personal data

21 / 40
Who has the legal obligation to keep records of processing activities?

A) The chief information officer
B) The chief privacy officer
C) The controller and processor
D) The data protection officer (DPO)

22 / 40
A North American organization based in the European Economic Area (EEA) processes personal data of natural persons. It processes ethnicity data on a large scale.

According to the GDPR, an organization is required to appoint a data protection officer (DPO) in three specific cases.

In this case, for what reason is it mandatory for this organization to appoint a DPO?

A) Foreigners' personal data are processed
B) Personal data are processed in a third country
C) Personal data of minorities are processed
D) Special categories of personal data are processed on a large scale

23 / 40
A data protection officer (DPO) works for the Ministry of Transportation, which is a national department.

A new project is announced to monitor people's driving behavior on the national highways. The Ministry wants to use an intelligent video analysis system to single out cars and automatically recognize license plates.

The state secretary is in a hurry to get the project started and worries that privacy issues might cause unwelcome delays.

What should the DPO do?

A) Ask the state secretary to contact the supervisory authority, because this is clearly outside the DPO's scope
B) Assure the state secretary that a data protection impact assessment (DPIA) is unnecessary, if data subjects are informed of the data processing
C) Inform the state secretary that a DPIA is mandatory for the large-scale monitoring of a public space
D) Urge the state secretary to reconsider the project because mass surveillance data processing is prohibited

24 / 40
Data protection officers (DPOs) are bound by secrecy or confidentiality concerning the performance of their tasks.

In relation to which party is the DPO **exempted** from this secrecy or confidentiality to seek advice?

A) The board of directors of the company
B) The data protection and privacy network members team
C) The information security officer (ISO)
D) The supervisory authority

25 / 40
A data protection impact assessment (DPIA) is a tool to identify data protection risks, especially the ones which are likely to highly affect the rights and freedoms of natural persons.

Why can the DPIA be seen as part of an organization's wider risk management?

A) Because the DPIA assesses all security risks of the organization under review and replaces any other risk assessment or risk management
B) Because the DPIA assesses risks by the likelihood and severity of the risk, similar to other well-defined components of risk management
C) Because the DPIA is mandatory for each project, according to the GDPR, which reduces all other legal requirements for risk management

26 / 40
According to the GDPR, what should always be part of a data protection impact assessment (DPIA)?

A) Develop a subject access request procedure to ensure compliance with data subjects' rights
B) Identify the personal data that are processed and the intended purposes of the processing
C) Notify the data subjects that an assessment will take place and request their explicit consent
D) Set up an incident response plan and define appropriate safeguards to avoid data breaches

27 / 40
An organization develops a new product to find underperforming employees. They search their internet history and analyze work behavior using artificial intelligence (AI).

Although the software engineers do not fully understand the algorithm, management decides to fire the bottom 10% employees.

The data protection officer (DPO) is concerned about the impact of this product and informs the board that a data protection impact assessment (DPIA) is required.

What is **not** part of the reason why a DPIA is mandatory?

A) The automation of the personal data processing
B) The evaluation that may affect the data subjects significantly
C) The processing of special categories of personal data
D) The systematic monitoring of personal aspects of natural persons

28 / 40
What is **not** an outcome of a data protection impact assessment (DPIA)?

A) A log of access to confidential data, with an automated authorization check
B) A record of data subjects' views on the intended processing operations
C) A systematic description of the intended processing operations
D) An assessment of risks to the rights and freedoms of data subjects

29 / 40
The GDPR details what the output of a data protection impact assessment (DPIA) must contain at a minimum.

What is **not** mandatory in a DPIA?

A) A description of the processing and its purposes
B) An assessment of the necessity and proportionality of the processing operations in relation to the purposes
C) An assessment of the risks to the rights and freedoms of data subjects
D) The advice of the supervisory authority

30 / 40
A data protection impact assessment (DPIA) shows that the intended processing involves collecting more data on individual customers than is necessary to achieve the intended purpose.

According to the GDPR, what is the **most** appropriate response?

A) Anonymize the data as soon as possible
B) Introduce a training and awareness program
C) Limit the period of time for which the data is stored
D) Reduce the amount of data collected

31 / 40
What is best done **first**, before starting a data protection impact assessment (DPIA)?

A) Determining measures to address the identified risks
B) Determining whether there is a need for a DPIA
C) Identifying the risks to the rights and freedoms of data subjects

32 / 40
A company performs a data protection impact assessment (DPIA).

Why is data mapping useful for a DPIA?

A) It assesses all organizational risks to privacy.
B) It helps to gain an overview of the personal data in use.
C) It helps to inform all relevant parties.

33 / 40
A privacy expert is hired by an organization. They wish to outsource part of their data processing activities. The expert performs a data protection impact assessment (DPIA) on the processing that involves a data processor.

One of the main steps of a DPIA requires the controller to provide all the input and does not require the processor to be involved.

Which step is that?

A) Assessment of the necessity and proportionality of the processing
B) Assessment of the risks to the rights and freedoms of data subjects
C) Mitigating measures to address the risks, including safeguards
D) Systematic descriptions of the intended processing operations

34 / 40
A large company is struggling financially. The board wants employees to work more efficiently.

The board starts an experiment in which the internet activities of the employees are monitored. The data are analyzed to see where more efficiency can be achieved. People categorized as *inefficient* might be dismissed.

Why must a data protection impact assessment (DPIA) be done before using the new procedure?

A) Because a large company has many employees. Therefore, the processing will be large scale.
B) Because it is an experiment. A DPIA is required for new and experimental processing activities.
C) Because it is systematic processing. The decisions might significantly affect the employees.

35 / 40
An organization plans to make automated decisions on its clients, based on profiling.

Which part of the data protection impact assessment (DPIA) needs extra attention?

A) The assessment of the need to perform a DPIA in relation to this processing activity
B) The measures to protect the rights of the data subject that will be implemented
C) The measures to secure the personal data from being requested by data subjects
D) The procedures for data erasure after a data subject asks for their data to be removed

36 / 40
The GDPR states that organizations must seek ways to prevent personal data breaches. Therefore, it is important to quickly recognize incidents that can be classified as personal data breaches.

According to the GDPR, which incident is **not** a personal data breach?

A) A patient is expecting a package containing medical equipment, but it is delivered to the wrong address.
B) An employee working at a mental health clinic has misplaced a set of patient files that cannot be retraced.
C) The accidental destruction of personal data by a fire or an earthquake in a data warehouse
D) The unauthorized disclosure of a company's confidential financial data regarding an intended acquisition

37 / 40
In which situation is it required to report a personal data breach to the supervisory authority?

A) If the organization cannot resolve the incident within a timeframe of 72 hours after it has occurred
B) In any situation where there is a security threat to the rights and freedom of natural persons
C) Only if the incident is recognized as a personal data breach within a timeframe of 72 hours
D) When a personal data breach is likely to result in a risk to the rights and freedom of natural persons

38 / 40
The head of the Human Resources (HR) department has lost a memory stick containing the personal information of 35 employees. The memory stick is protected by strong encryption. The HR department also has this personal information stored in a backup device.

According to the GDPR, is it mandatory to report this personal data breach to the supervisory authority?

A) Yes, because all security incidents must be reported to the supervisory authority.
B) Yes, because reporting it enables the supervisory authority to inform the employees.
C) No, because it is not a legitimate interest of the company to report data breaches.
D) No, because this personal data breach creates no risk to the data subjects' rights.

39 / 40
According to the GDPR, in which situation must a personal data breach be reported to the data subjects affected?

A) When a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject
B) When the supervisory authority has determined that consent was the only legal ground for processing
C) When there is a security incident that is labelled as a personal data breach within 72 hours
D) When personal data is compromised by external factors such as hackers or other cyber criminals

40 / 40
In the best practice incident response process the phases prepare, respond and follow-up are defined. For each phase, documentation is essential.

In the respond phase, it is important to gather and preserve evidence to show why an incident happened and why the organization was not able to prevent the incident.

What must be gathered and preserved?

A) Audit control plans
B) Data protection impact assessments (DPIAs)
C) Evidence to provide a clear picture
D) System recovery plans

Answer Key

1 / 40
A company implements a privacy policy, which helps to demonstrate compliance with the GDPR. It is recommended that this policy is made publicly accessible for several reasons.

What is the **main** reason for making the privacy policy publicly available?

A) To allow customers and partners to verify which personal data the organization must process
B) To allow customers, partners and the supervisory authority to assess how personal data are handled
C) To communicate the result of data protection impact assessments (DPIAs) performed in the organization
D) To inform the supervisory authority of how the organization will respond after personal data breaches

A) Incorrect. Publicly available privacy policies do not establish which personal data must be processed by the organization. They provide transparency to the personal data processing.
B) Correct. A publicly available policy supports transparency, allows customers and partners to assess it, and provides a clear statement that supervisory authorities and other regulators can assess the organization against. (Literature: A, Chapter 16)
C) Incorrect. The result of the DPIAs are intended to be documented for internal consultation and should not be included in the privacy policy.
D) Incorrect. How the organization responds to a data breach is part of the data breach response plan, which is an internal document and not required to be publicly available.

2 / 40
According to the GDPR, what information is **not** a mandatory part of a privacy policy?

A) Information about international transfers of personal data to a third country
B) Information about the identity and contact details of the controller
C) Information relating to data security measures in the organization
D) Information relating to retention periods and data subject's rights

A) Incorrect. This is mandatory.
B) Incorrect. This is mandatory.
C) Correct. This is part of an information security policy. (Literature: A, Chapter 16; GDPR Article 13)
D) Incorrect. This is mandatory.

3 / 40
The GDPR embraces the principles of privacy by design and by default. The application of these principles includes the implementation of both technical and organizational measures.

Why are organizational measures necessary?

A) Because privacy by design and by default requires that the organization restricts personal data access to controllers only
B) Because protecting the rights of data subjects, requires organizational processes that technical measures cannot cover
C) Because the designation of a data protection officer (DPO), where mandatory, is regarded as an organizational measure

A) Incorrect. Organizational measures are meant to protect the data subjects' rights and consist of procedures for fair and transparent processing.
B) Correct. Some internal processes and procedures must be addressed by organizational measures to guarantee that the data subjects rights can be fully exercised in compliance with the GDPR. Technical tools and systems complement the organizational measures, but do not substitute them. (Literature: A, Chapter 9)
C) Incorrect. Organizational measures are meant to protect the data subjects' rights and consist of procedures for fair and transparent processing.

4 / 40
A company is setting up a project to create a new, free service for consumers.

According to privacy by design, what is the **most** desirable time to discuss data protection?

A) From the start of the project
B) During the implementation phase
C) When the project nears completion

A) Correct. Privacy and data protection must be promoted from the start of the project in line with the privacy by design principle. (Literature: A, Chapter 5; F)
B) Incorrect. Discussing data protection in the implementation phase is too late.
C) Incorrect. Discussing data protection in the project completion phase is too late.

5 / 40
An organization is implementing the privacy information management system (PIMS) using the ISO/IEC 27701 standard.

During the implementation, some of the organization's contractors realize that they must comply with several legal requirements from different countries. The contractors decide to ask the data protection officer (DPO) for advice.

According to ISO/IEC 27701, how should the DPO categorize the legal requirements?

A) Internal issue because the legal requirements directly impact the PIMS, which is an internal matter.
B) Internal issue because the relevant factors are the contractors who must be seen as coworkers.
C) External issue because the contractors operate outside the regular coworkers of the organization.
D) External issue because the legal requirements are relevant but independent from the organization.

A) Incorrect. Although the legal requirements will likely directly impact the PIMS, the legal requirements themselves are always external issues.
B) Incorrect. Although contractors must indeed be seen as coworkers and staff management and reporting are internal issues, the factors to be categorized are the legal requirements.
C) Incorrect. All coworkers, including external contractors, their management and reporting must be considered internal issues. Additionally, the factors to be categorized are the legal requirements, which are external issues.
D) Correct. According to the term introduced by ISO/IEC 27701, legal requirements are considered external issues. (Literature: B, Chapter 2)

6 / 40
A business to consumer (B2C) organization is implementing a privacy information management system (PIMS).

The data protection officer (DPO) comes across the following media that contain information:

- An **external hard drive** with competitor information and a description of their strengths and weaknesses.
- Some **paper files** from human resources (HR) with health information and emergency contact information in them.
- A computer **server** which contains a backup of all customer data, including of direct consumers.
- Old **USB drives** with former coworkers' personal information and their last salaries at the organization.

Which media do **not** have to be part of the PIMS?

A) External hard drive
B) Paper files
C) Server
D) USB drives

A) Correct. The PIMS should be concerned with personal information and in this case the external hard drive does not contain any personal information. (Literature: B, Chapter 1)
B) Incorrect. All media, even non-digital media, that contain personal information should be part of the PIMS. The HR files contain personal information and must be in the PIMS.
C) Incorrect. All media, even if they only contain a backup, that contain personal information should be part of the PIMS. The server contains consumer data, which is data from natural persons and, therefore, personal information.
D) Incorrect. All media that contain personal information should be part of the PIMS, even if the information is of former coworkers.

7 / 40
When defining a privacy information management system (PIMS), different documents are created. One of these documents is the statement of applicability (SoA).

What is a statement of applicability (SoA)?

A) The SoA gauges how likely it is that processing data results in a high risk to individuals.
B) The SoA records where and how personal data of employees and customers is processed.
C) The SoA states which controls must be applied to manage or minimize risk within the PIMS.

A) Incorrect. This is what the data protection impact assessment (DPIA) does.
B) Incorrect. This is recorded in the recording of processing activities (ROPA).
C) Correct. According to ISO/IEC 27701, this is the definition of an SoA. (Literature: B, Chapter 4)

8 / 40
It is fundamental to a privacy information management system (PIMS), both in the short and long term, to be able to demonstrate how corporate policies, operating procedures, and work instructions are formulated. This ensures that actions are traceable to management decisions and policies, and that the results are reproducible.

Which requirement of the PIMS is this referring to?

A) Audit
B) Documentation
C) Management review
D) Statement of applicability (SoA)

A) Incorrect. A management system audit program has the main objective to monitor conformity between the management system requirements and working practices.
B) Correct. It is likely that the organization will find it useful to keep records of developments and activities upon which it can call should it need to in the future. Many of these items are recorded and the organization retains the data for as long as necessary. Creating records of operating activities for the purpose of review and decision making is also relevant. (Literature: B, Chapter 3)
C) Incorrect. Management review is a procedure in which top management reviews the progress of the PIMS from its inception to operation. This procedure ensures that the PIMS' progress is effective and meets corporate requirements over time.
D) Incorrect. The SoA is a document that details which controls are applied within the PIMS and which are not.

9 / 40
Why should top management review the progress of the privacy information management system (PIMS)?

A) To ensure that the PIMS conforms with all relevant legal requirements
B) To ensure that the PIMS has enough privacy controls to mitigate risks
C) To ensure that the PIMS is audited regularly and is producing documents
D) To ensure that the PIMS is effective and meets corporate requirements

A) Incorrect. This is a responsibility within the PIMS, not the purpose of the management review.
B) Incorrect. This is a responsibility within the PIMS, not the purpose of the management review.
C) Incorrect. This is a responsibility within the PIMS, not the purpose of the management review.
D) Correct. It is appropriate that top management reviews the progress of the PIMS from its inception through to operation, ensuring that it is effective and meets corporate requirements over time. (Literature: B, Chapter 3)

10 / 40
Auditing the privacy information management system (PIMS) can be done for multiple reasons.

According to ISO/IEC 27701, what is the **main** objective of PIMS audits?

A) To confirm that requirements of the relevant national and international standards are maintained
B) To identify specific areas of concern and address the selection of individual work processes
C) To include updates of relevant changes to legislation and regulations, and their interpretation
D) To monitor conformity between the management system requirements and working practices

A) Incorrect. Confirming the requirements of the applicable international standards is part of the objectives, but the main objective is to monitor conformity between the management system requirements and working practices.
B) Incorrect. This is part of the improvements that audit can provide, but this is not a main objective.
C) Incorrect. This is part of the improvement opportunities that audit can provide, but this is not a main objective.
D) Correct. The main objective of a management system audit program is to monitor conformity between the management system requirements and working practices. (Literature: B, Chapter 3)

11 / 40
An organization implements a privacy information management system (PIMS). The specific requirements must be based on local rules and contractual requirements.

What should be the next step for the organization's legal team?

A) Hire local legal advice and guidance, and apply the ISO/IEC 27701 as the contractual standard to clients and suppliers
B) Look up the applicable international best practices, and review all contracts which involve personal data processing
C) Map the applicable legislation and related legal sanctions, and review all contracts which involve personal data processing
D) Request local supervisory authority's guidance, and apply the ISO/IEC 27701 as a contractual standard to clients and suppliers

A) Incorrect. The specific requirements of a PIMS need to be determined considering the appropriate local rules and contractual requirements. There may be no need to request local legal advice if the legal team is already familiar with the local legislation, and not all contracts will necessarily have the ISO/IEC 27701 as contractual standard requirements.
B) Incorrect. The specific requirements of a PIMS must be determined considering contractual requirements and the applicable local legislation, not international best practices.
C) Correct. The specific requirements of a PIMS need to be determined considering the appropriate local rules and contractual requirements. (Literature: B, Chapter 4)
D) Incorrect. The specific requirements of a PIMS need to be determined considering the appropriate local rules and contractual requirements. There is no need to request the local supervisory authority's guidance, and not all contracts will necessarily have the ISO/IEC 27701 as contractual standard requirements.

12 / 40
An organization is merging with another company. The organization already has a privacy information management system (PIMS).

The completion of the process depends on demonstrating that all the personal data processing operations follow the ISO/IEC 27701 and the applicable legislation.

What is the **most** appropriate means to show this?

A) A data protection impact assessment (DPIA) report
B) A privacy impact assessment (PIA) report
C) A recent PIMS audit report
D) A statement of applicability (SoA) report

A) Incorrect. A DPIA report registers a risk assessment typically undertaken before the implementation of a project. A DPIA is required for processing that is likely to result in a high risk to individuals.
B) Incorrect. A PIA report registers a risk assessment typically undertaken before the implementation of a project. A DPIA is required for processing that is likely to result in a high risk to individuals.
C) Correct. Audit reports identify conformity and non-conformity between the actual practice and the requirements. (Literature: B, Chapter 3)
D) Incorrect. The statement of applicability (SoA) (a statement, not a report) is a document that details which controls are applied within the PIMS and which are not, but there is no guarantee that it reflects the actual practice. It also does not guarantee legal compliance.

13 / 40
A small organization has developed a successful software service. Their service is a large success, which means the organization needs a more robust cloud solution. Therefore, the organization must select an external cloud supplier.

The organization is ISO/IEC 27701 certified. When searching for a supplier, the organization comes across several cloud suppliers. Some suppliers are ISO/IEC 27701 certified, but others are not.

How can an ISO/IEC 27701 certification help with supplier selection?

A) The ISO/IEC 27701 certification of a supplier includes a cost/benefit analysis, which ensures lower costs for services.
B) The ISO/IEC 27701 certification of a supplier lowers the need for supplier audits, which is easier for the organization.
C) The ISO/IEC 27701 certification of the organization has procedures for data processing, which extends to any supplier.
D) The ISO/IEC 27701 certification of the organization requires an ISO/IEC 27701 certified supplier, which limits choices.

A) Incorrect. An ISO/IEC 27701 certification does not include a list of suppliers. Since the controller is always responsible for ensuring data protection, they should audit suppliers. ISO/IEC 27701 certified suppliers already have been audited.
B) Correct. An ISO/IEC 27701 certified supplier is more likely to process personal data responsibly and to be able to cooperate more effectively after a personal data breach. (Literature: B, Chapter 5)
C) Incorrect. The controller will always remain responsible for ensuring data protection, which means they should audit suppliers. ISO/IEC 27701 certified suppliers already have been audited.
D) Incorrect. An ISO/IEC 27701 certification does not require all suppliers to have the same certification. Because the controller will always remain responsible for ensuring data protection, they should audit suppliers. ISO/IEC 27701 certified suppliers already have been audited.

14 / 40
When working towards ISO/IEC 27701 certification, there are several management systems involved. Two of these systems are:

- the privacy information management system (PIMS)
- the information security management system (ISMS)

What is true about these systems?

A) The ISMS and PIMS audits may be combined or done separately, even though the PIMS requirements depend on the maintenance of the ISMS.
B) The ISMS and PIMS audits must never be done together, because the PIMS and ISMS system requirements do not depend on each other.
C) The ISMS is part of the PIMS and addresses information protection, since the ISMS looks at a business risk approach to personal data.

A) Correct. The two audits may be combined. ISO/IEC 27701 certification depends in part on ISO/IEC 27001 certifications and audits. (Literature B, Chapter 6)
B) Incorrect. The two audits may be combined or done separately. ISO/IEC 27701 certification depends in part on ISO/IEC 27001 certifications and audits.
C) Incorrect. The ISMS is meant to get an idea of the risks to all data in general in the organization and mitigate those risks through the controls in the ISMS. The ISMS does not specifically focus on personal data.

15 / 40
An organization is implementing a privacy information management system (PIMS). The GDPR requires that “personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data […]”.

What is the relationship between this requirement and the ISO/IEC 27701 standard?

A) The GDPR principles of integrity and confidentiality form the foundation of the PIMS that is required for the ISO/IEC 27701 standard.
B) The GDPR principles of lawfulness, fairness, and transparency contribute to the PIMS and the information security management system (ISMS).
C) The GDPR principle of purpose limitation prescribes exactly how the data that fall under the PIMS may or may not be used.
D) The GDPR principle of storage limitation explains the length of time the personal data reside in the PIMS before processing.

A) Correct. The data security principle is an essential condition for a PIMS and the GDPR principles that determine what is appropriate security of personal data is called ‘integrity and confidentiality’. Therefore, these principles are the foundation of the PIMS. (Literature: B, Chapter 3 and GDPR, Art. 5.1.f)
B) Incorrect. The PIMS may contribute to the ‘lawfulness, fairness and transparency’, but the ‘integrity and confidentiality’ principle is the foundation for the PIMS. Therefore, the latter is the one which best relates to the PIMS.
C) Incorrect. The PIMS may contribute to the ‘purpose limitation’, but the ‘integrity and confidentiality’ principle is the foundation for the PIMS. Therefore, the latter is the one which best relates to the PIMS.
D) Incorrect. The PIMS may contribute to the ‘storage limitation’, but the ‘integrity and confidentiality’ principle is the foundation for the PIMS. Therefore, the latter is the one which best relates to the PIMS.

16 / 40
The ISO/IEC 27701 standard contains a chapter dedicated to additional guidance that aligns with the ISO/IEC 27002 standard.

What type of recommendations are **not** included in this chapter?

A) Develop privacy policies separate from or combined with information security policies
B) Ensure at least awareness training for all coworkers that handle or process personal data
C) Label all data clearly to identify where personal data is stored or otherwise processed
D) Plan internal and external audits with a specific interval depending on the audit scope

A) Incorrect. The recommendation on developing privacy policies is a part of this chapter.
B) Incorrect. The recommendation of ensuring at least some training is in this chapter.
C) Incorrect. The recommendation to label all data clearly is part of this chapter.
D) Correct. Although the ISO/IEC 27701 standard does not specifically deal with compliance and audits, the standard is developed to align with ISO/IEC 27001 and ISO/IEC 27002, which do contain these categories. (Literature B, Chapter 5)

17 / 40
Applying privacy information management system (PIMS) controls to manage risk is not an easy task, and it is recommended to go through all the stages.

The first stage is to design a set of controls to manage risks. The other stages are listed below (in random order):

1. Compare controls to ISO/IEC 27701's Annex A or B
2. Produce the statement of applicability (SoA)
3. Effectively implement the controls

What is the **correct** order of the other stages?

A) 1, 2, 3
B) 1, 3, 2
C) 2, 1, 3
D) 2, 3, 1

A) Incorrect. The correct order is 1, 3, 2.
B) Correct. After a set of controls is designed, the controls must be compared to ISO/IEC 27701's Annexes to ensure the required level of assurance against privacy risks. Then the controls should be implemented and the SoA follows last. (Literature: B, Chapter 4)
C) Incorrect. The correct order is 1, 3, 2.
D) Incorrect. The correct order is 1, 3, 2.

18 / 40
According to the GDPR, which activity is always a responsibility of the controller?

A) Being responsible for performing a data protection impact assessment (DPIA)
B) Contracting a security company for the protection of personal data in transit
C) Implementing a new method to collect personal data from the customers
D) Maintaining records of the processing activities carried out by the processor

A) Correct. Responsibility for DPIAs falls to the controller and should not be outsourced to a data processor. (Literature: A, Chapter 12; GDPR Article 35)
B) Incorrect. This could be the responsibility of the processor, if prior written authorization exists.
C) Incorrect. This could be the responsibility of the processor, if prior written authorization exists.
D) Incorrect. This element is the responsibility of the processor. The controller maintains a record of the processing activities they control.

19 / 40
A hospital outsources its printing of patient invoices to a printing company. The printing company also prints invoices for other organizations.

Due to an error, names and addresses were mixed up when they were sorted at the printing company, and a number of invoices were sent to the wrong patients.

The hospital had carefully analyzed their own processes. The hospital had a robust verification process in place and has contractual agreements with the printing company.

Why will the hospital be held **responsible** by the supervisory authority?

A) Because the contract determines this
B) Because the hospital is the controller
C) Because the mix-up is between patients
D) Because the verification has gone wrong

A) Incorrect. The hospital is accountable because, as the controller, it is subject to the accountability principle, determined by the GDPR.
B) Correct. The GDPR states that "The controller shall be responsible […], paragraph 1('accountability')" for the lawfulness of processing. The controller will be held responsible and accountable by the supervisory authority, whatever contract may be in place between controller and processor. The controller should only use processors that provide sufficient guarantees that they implement appropriate technical and organizational measures. (Literature: A, Chapter 12; GDPR, article 5 (2))
C) Incorrect. It does not matter that the data subjects all belong to the same controller. Who is the controller is relevant here.
D) Incorrect. There is nothing to indicate the verification went wrong. The supervisory authority will always hold the controller responsible.

20 / 40
When a controller and a processor sign a contract for the processing of personal data, they both have specific responsibilities. Some of these responsibilities are prescribed by the GDPR and others can be arranged in the contract.

According to the GDPR, when does the processor always need written authorization by the controller?

A) When the processor contracts a company to protect data during transfers
B) When the processor contracts a third party to process personal data
C) When the processor implements a new method to collect personal data
D) When the processor implements a new method to delete personal data

A) Incorrect. This element is or might be at the determination of the processor according to the contract, as it is not clearly defined by the GDPR.
B) Correct. This engaging of another processor cannot be done without the prior specific or general written authorization of the controller. (Literature: A, Chapter 12; GDPR Article 28(2))
C) Incorrect. This element is or might be at the determination of the processor according to the contract, as it is not clearly defined by the GDPR.
D) Incorrect. This element is or might be at the determination of the processor according to the contract, as it is not clearly defined by the GDPR.

21 / 40
Who has the legal obligation to keep records of processing activities?

A) The chief information officer
B) The chief privacy officer
C) The controller and processor
D) The data protection officer (DPO)

A) Incorrect. The chief information officer has the overall responsibility for information technology and information management.
B) Incorrect. The chief privacy officer should create engagement for GDPR compliance within the organization.
C) Correct. Both controller and processor are required to keep a record of all processing activities. (Literature: A, Chapter 12; GDPR Article 30)
D) Incorrect. Although in practice it is the DPO that creates inventories, holds a register of processing activities and has been given the responsibility to maintain these records, this is done under the legal obligation of the controller or processor.

22 / 40
A North American organization based in the European Economic Area (EEA) processes personal data of natural persons. It processes ethnicity data on a large scale.

According to the GDPR, an organization is required to appoint a data protection officer (DPO) in three specific cases.

In this case, for what reason is it mandatory for this organization to appoint a DPO?

A) Foreigners' personal data are processed
B) Personal data are processed in a third country
C) Personal data of minorities are processed
D) Special categories of personal data are processed on a large scale

A) Incorrect. This is not one of the three basic conditions specified in the GDPR.
B) Incorrect. This is not one of the three basic conditions specified in the GDPR.
C) Incorrect. This is not one of the three basic conditions specified in the GDPR.
D) Correct. This is one of the cases specified in the GDPR, when the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9. Ethnic or racial data is specifically mentioned in Article 9 of the GDPR. The other two conditions are: (1) processing is carried out by a public authority or body, except for courts acting in their judicial capacity, (2) processing that requires regular and systematic monitoring of data subjects on a large scale. These three basic conditions apply to both controllers and processors. (Literature: A, Chapter 2; GDPR Article 9 and Article 37)

23 / 40
A data protection officer (DPO) works for the Ministry of Transportation, which is a national department.

A new project is announced to monitor people's driving behavior on the national highways. The Ministry wants to use an intelligent video analysis system to single out cars and automatically recognize license plates.

The state secretary is in a hurry to get the project started and worries that privacy issues might cause unwelcome delays.

What should the DPO do?

A) Ask the state secretary to contact the supervisory authority, because this is clearly outside the DPO's scope
B) Assure the state secretary that a data protection impact assessment (DPIA) is unnecessary, if data subjects are informed of the data processing
C) Inform the state secretary that a DPIA is mandatory for the large-scale monitoring of a public space
D) Urge the state secretary to reconsider the project because mass surveillance data processing is prohibited

A) Incorrect. A DPO should be sufficiently qualified to discuss this.
B) Incorrect. Informing data subjects will not exempt an organization from the responsibility to do a DPIA.
C) Correct. The project demands systematic monitoring of a publicly accessible area on a large scale, and this is one of the three mandatory scenarios for performing a DPIA. (Literature: A, Chapter 5; GDPR Article 35(3)(c))
D) Incorrect. Monitoring, surveillance and profiling are not prohibited, as long as people's rights and freedoms are sufficiently protected.

24 / 40
Data protection officers (DPOs) are bound by secrecy or confidentiality concerning the performance of their tasks.

In relation to which party is the DPO **exempted** from this secrecy or confidentiality to seek advice?

A) The board of directors of the company
B) The data protection and privacy network members team
C) The information security officer (ISO)
D) The supervisory authority

A) Incorrect. Being easily accessible does not mean that the DPO should ask for advice of board members. The DPO should fulfill an independent role.
B) Incorrect. Being easily accessible does not mean that the DPO should ask for advice of the data protection and privacy network members' team.
C) Incorrect. Being easily accessible does not mean that the DPO should ask for advice of the ISO.
D) Correct. The obligation of secrecy and or confidentiality does not prohibit the DPO from contacting and seeking advice from the supervisory authority. (Literature: A, Chapter 2; GDPR Article 36 and Article 39(1)(e))

25 / 40
A data protection impact assessment (DPIA) is a tool to identify data protection risks, especially the ones which are likely to highly affect the rights and freedoms of natural persons.

Why can the DPIA be seen as part of an organization's wider risk management?

A) Because the DPIA assesses all security risks of the organization under review and replaces any other risk assessment or risk management
B) Because the DPIA assesses risks by the likelihood and severity of the risk, similar to other well-defined components of risk management
C) Because the DPIA is mandatory for each project, according to the GDPR, which reduces all other legal requirements for risk management

A) Incorrect. A DPIA only focuses on personal data protection and privacy risks.
B) Correct. This is the link between DPIA and risk management. (Literature: A, Chapter 2; GDPR Recital 90)
C) Incorrect. A DPIA is not always required and it does not diminish needs for other risk management.

26 / 40
According to the GDPR, what should always be part of a data protection impact assessment (DPIA)?

A) Develop a subject access request procedure to ensure compliance with data subjects' rights
B) Identify the personal data that are processed and the intended purposes of the processing
C) Notify the data subjects that an assessment will take place and request their explicit consent
D) Set up an incident response plan and define appropriate safeguards to avoid data breaches

A) Incorrect. This is a possible measure, based on the outcome of a DPIA.
B) Correct. Every DPIA should start with a description of the intended processing and the purposes of the processing. (Literature: A, Chapter 8; GDPR, Article 35(7)(a))
C) Incorrect. Consent is not required to do a DPIA.
D) Incorrect. This is a possible measure, based on the outcome of a DPIA.

27 / 40
An organization develops a new product to find underperforming employees. They search their internet history and analyze work behavior using artificial intelligence (AI).

Although the software engineers do not fully understand the algorithm, management decides to fire the bottom 10% employees.

The data protection officer (DPO) is concerned about the impact of this product and informs the board that a data protection impact assessment (DPIA) is required.

What is **not** part of the reason why a DPIA is mandatory?

A) The automation of the personal data processing
B) The evaluation that may affect the data subjects significantly
C) The processing of special categories of personal data
D) The systematic monitoring of personal aspects of natural persons

A) Incorrect. This is a reason for a DPIA being mandatory.
B) Incorrect. This is a reason for a DPIA being mandatory.
C) Correct. While the system will be collecting personal data, these data are not considered special categories of data. (Literature: A, Chapter 8; GDPR Article 35)
D) Incorrect. This is a reason for a DPIA being mandatory.

28 / 40
What is **not** an outcome of a data protection impact assessment (DPIA)?

A) A log of access to confidential data, with an automated authorization check
B) A record of data subjects' views on the intended processing operations
C) A systematic description of the intended processing operations
D) An assessment of risks to the rights and freedoms of data subjects

A) Correct. This is not an outcome of a DPIA, but is an ongoing activity performed by information security. (Literature: A, Chapter 8 and Chapter 3; GDPR Article 35)
B) Incorrect. This is a possible outcome of the DPIA.
C) Incorrect. This is a possible outcome of the DPIA.
D) Incorrect. This is a possible outcome of the DPIA.

29 / 40
The GDPR details what the output of a data protection impact assessment (DPIA) must contain at a minimum.

What is **not** mandatory in a DPIA?

A) A description of the processing and its purposes
B) An assessment of the necessity and proportionality of the processing operations in relation to the purposes
C) An assessment of the risks to the rights and freedoms of data subjects
D) The advice of the supervisory authority

A) Incorrect. This is a mandatory part of the DPIA.
B) Incorrect. This is a mandatory part of the DPIA.
C) Incorrect. This is a mandatory part of the DPIA.
D) Correct. It is not always mandatory to consult with the supervisory authority, and it is not mandatory to include a log of the advice in the DPIA. (Literature: A, Chapter 5; GDPR Article 35(7) and Article 36(1))

30 / 40
A data protection impact assessment (DPIA) shows that the intended processing involves collecting more data on individual customers than is necessary to achieve the intended purpose.

According to the GDPR, what is the **most** appropriate response?

A) Anonymize the data as soon as possible
B) Introduce a training and awareness program
C) Limit the period of time for which the data is stored
D) Reduce the amount of data collected

A) Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place.
B) Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place.
C) Incorrect. This is a mitigating risk measure, but the unnecessary data are not allowed to be processed in the first place
D) Correct. This implements the principle of data minimization and reduces the risks for the data subjects. (Literature: A, Chapter 8; GDPR 5(1))

31 / 40
What is best done **first**, before starting a data protection impact assessment (DPIA)?

A) Determining measures to address the identified risks
B) Determining whether there is a need for a DPIA
C) Identifying the risks to the rights and freedoms of data subjects

A) Incorrect. This is part of a DPIA and done after determining the need for one.
B) Correct. The organization needs to determine whether the law requires a DPIA or if the needs of the organization demand one. (Literature: A, Chapter 5; GDPR Article 35(7))
C) Incorrect. This is part of a DPIA and done after determining the need for one.

32 / 40
A company performs a data protection impact assessment (DPIA).

Why is data mapping useful for a DPIA?

A) It assesses all organizational risks to privacy.
B) It helps to gain an overview of the personal data in use.
C) It helps to inform all relevant parties.

A) Incorrect. Data mapping does not assess risks.
B) Correct. Data mapping identifies data in use. Mapped data flows help to identify potential risks that must be assessed. (Literature: A, Chapter 7)
C) Incorrect. Data mapping is not used to inform parties.

33 / 40
A privacy expert is hired by an organization. They wish to outsource part of their data processing activities. The expert performs a data protection impact assessment (DPIA) on the processing that involves a data processor.

One of the main steps of a DPIA requires the controller to provide all the input and does not require the processor to be involved.

Which step is that?

A) Assessment of the necessity and proportionality of the processing
B) Assessment of the risks to the rights and freedoms of data subjects
C) Mitigating measures to address the risks, including safeguards
D) Systematic descriptions of the intended processing operations

A) Correct. This is the responsibility of the controller and does not involve the processor. (Literature: A, Chapter 12)
B) Incorrect. Input is needed from the processor on potential risks.
C) Incorrect. Input is needed on the mitigating measures taken by the processor.
D) Incorrect. To make a full description, input from the processor is needed.

34 / 40
A large company is struggling financially. The board wants employees to work more efficiently.

The board starts an experiment in which the internet activities of the employees are monitored. The data are analyzed to see where more efficiency can be achieved. People categorized as *inefficient* might be dismissed.

Why must a data protection impact assessment (DPIA) be done before using the new procedure?

A) Because a large company has many employees. Therefore, the processing will be large scale.
B) Because it is an experiment. A DPIA is required for new and experimental processing activities.
C) Because it is systematic processing. The decisions might significantly affect the employees.

A) Incorrect. The large scale may be of influence but is not a criterion by its own. Large scale monitoring in a public space would be a criterion. However, the company is not a public space.
B) Incorrect. It is irrelevant whether it concerns an experiment or an ordinary processing activity.
C) Correct. This is defined as one of the three cases in which a DPIA is mandatory. (Literature: A, Chapter 5; GDPR Article 35(3)(b))

35 / 40
An organization plans to make automated decisions on its clients, based on profiling.

Which part of the data protection impact assessment (DPIA) needs extra attention?

A) The assessment of the need to perform a DPIA in relation to this processing activity
B) The measures to protect the rights of the data subject that will be implemented
C) The measures to secure the personal data from being requested by data subjects
D) The procedures for data erasure after a data subject asks for their data to be removed

A) Incorrect. For processing activities involving automated decision making, including profiling, a DPIA is always required.
B) Correct. The risks automated decision-making brings with it need special attention. How to mitigate the risk should be carefully described. A mitigation could be to allow human intervention. (Literature: A, Chapter 5; GDPR Article 35)
C) Incorrect. Data need to be secured in general, but data subjects have the right of access.
D) Incorrect. This is part of a DPIA, but it is not most appropriate for specific attention if automated decisions are made.

36 / 40
The GDPR states that organizations must seek ways to prevent personal data breaches. Therefore, it is important to quickly recognize incidents that can be classified as personal data breaches.

According to the GDPR, which incident is **not** a personal data breach?

A) A patient is expecting a package containing medical equipment, but it is delivered to the wrong address.
B) An employee working at a mental health clinic has misplaced a set of patient files that cannot be retraced.
C) The accidental destruction of personal data by a fire or an earthquake in a data warehouse
D) The unauthorized disclosure of a company's confidential financial data regarding an intended acquisition

A) Incorrect. This is a personal data breach involving special category personal data.
B) Incorrect. The accidental loss of any personal data, and especially special category personal data, is also considered a personal data breach.
C) Incorrect. Even if the incident is caused by a natural disaster or force majeure, this must be considered a personal data breach.
D) Correct. This is a data breach, but no personal data are compromised. It is not a personal data breach. (Literature: A, Chapter 3; GDPR Article 4(12))

37 / 40
In which situation is it required to report a personal data breach to the supervisory authority?

A) If the organization cannot resolve the incident within a timeframe of 72 hours after it has occurred
B) In any situation where there is a security threat to the rights and freedom of natural persons
C) Only if the incident is recognized as a personal data breach within a timeframe of 72 hours
D) When a personal data breach is likely to result in a risk to the rights and freedom of natural persons

A) Incorrect. The timeframe in which the incident is resolved is unimportant.
B) Incorrect. A threat is not enough. A notification is only mandatory when a personal data breach occurred, that is likely to result in a risk to the rights and freedoms of natural persons.
C) Incorrect. The incident management process may be unable to identify the incident within 72 hours. The GDPR states that personal data breaches must be reported "without undue delay and where feasible not later than 72 hours after having become aware of it".
D) Correct. Notification to the supervisory authority is mandatory for incidents involving personal data, that are likely to result in a risk to the rights and freedoms of natural persons. (Literature: A, Chapter 14; GDPR Article 33(1))

38 / 40
The head of the Human Resources (HR) department has lost a memory stick containing the personal information of 35 employees. The memory stick is protected by strong encryption. The HR department also has this personal information stored in a backup device.

According to the GDPR, is it mandatory to report this personal data breach to the supervisory authority?

A) Yes, because all security incidents must be reported to the supervisory authority.
B) Yes, because reporting it enables the supervisory authority to inform the employees.
C) No, because it is not a legitimate interest of the company to report data breaches.
D) No, because this personal data breach creates no risk to the data subjects' rights.

A) Incorrect. Only personal data breaches that result in a high risk to the rights of data subject must be reported. Although it can be good practice to report all personal data breaches to avoid breaking the law, this is not mandatory.
B) Incorrect. The data subjects' rights are not at risk, so they do not need to be informed. It is not the supervisory authority's task to inform the data subjects.
C) Incorrect. The legitimate interest of the company is a legal ground for processing. It does not relate to personal data breaches and how these must be reported.
D) Correct. The strong encryption and backup are enough to guarantee the confidentiality and availability of the personal data. Therefore, this data breach is unlikely to result in a risk to the rights and freedoms of natural persons. It is not mandatory to report this data breach to the supervisory authority. (Literature: A, Chapter 14; GDPR Article 33(1))

39 / 40
According to the GDPR, in which situation must a personal data breach be reported to the data subjects affected?

A) When a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject
B) When the supervisory authority has determined that consent was the only legal ground for processing
C) When there is a security incident that is labelled as a personal data breach within 72 hours
D) When personal data is compromised by external factors such as hackers or other cyber criminals

A) Correct. Data subjects should be informed if the personal data breach poses a high risk to their rights and freedoms. (Literature: A, Chapter 14; GDPR Article 34(1))
B) Incorrect. Only personal data breaches that pose a high risk must also be reported to the data subjects.
C) Incorrect. The 72 hours are the timeframe within which the personal data breach should be reported to the supervisory authority. Not all personal data breaches must be reported to the data subjects.
D) Incorrect. Notification does not depend on the underlying cause of the personal data breach.

40 / 40
In the best practice incident response process the phases prepare, respond and follow-up are defined. For each phase, documentation is essential.

In the respond phase, it is important to gather and preserve evidence to show why an incident happened and why the organization was not able to prevent the incident.

What must be gathered and preserved?

A) Audit control plans
B) Data protection impact assessments (DPIAs)
C) Evidence to provide a clear picture
D) System recovery plans

A) Incorrect. An audit control plan is not documented in the incident response process.
B) Incorrect. A DPIA is not documented in the incident response process.
C) Correct. Throughout the incident response process, evidence should be gathered and preserved to provide a clear picture of what happened and why the organization was unable to prevent the incident. (Literature: A, Chapter 14)
D) Incorrect. A system recovery plan is not documented in the incident response process.

Evaluation

The table below shows the correct answers to the questions in this sample exam.

Question	Answer	Question	Answer
1	B	**21**	C
2	C	**22**	D
3	B	**23**	C
4	A	**24**	D
5	D	**25**	B
6	A	**26**	B
7	C	**27**	C
8	B	**28**	A
9	D	**29**	D
10	D	**30**	D
11	C	**31**	B
12	C	**32**	B
13	B	**33**	A
14	A	**34**	C
15	A	**35**	B
16	D	**36**	D
17	B	**37**	D
18	A	**38**	D
19	B	**39**	A
20	B	**40**	C

Contact EXIN

www.exin.com