



CIPM^{Q&As}

Certified Information Privacy Manager

Pass IAPP CIPM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/cipm.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1**

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

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

QUESTION 2

SCENARIO

Please use the following to answer the next QUESTION:

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

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

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

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

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

Correct Answer: B

QUESTION 3

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

QUESTION 4



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: B

QUESTION 5

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

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

Correct Answer: C

[CIPM PDF Dumps](#)

[CIPM Practice Test](#)

[CIPM Study Guide](#)