CASE STUDY

Wonderwheels is a major national retailer specializing in outdoor sports, hunting, fishing and camping, including a wide variety of all-terrain vehicles (ATVs), which inspired its name. The company has operations currently based in the United States and has a long-term business plan to expand its retail centers to selected parts of the European Union (EU).

As part of ongoing current operations, management has asked an internal IS auditor to review the company's readiness for complying with requirements for protecting cardholder information. This is meant to be a high-level overview of where the firm stands and not a point-by-point review of its compliance with the specific standard (which would be undertaken as a separate engagement later in the year).

During the initial assessment, the IS auditor learned the following information:

- **Point-of-sale (POS) register encryption**—The retailer uses wireless POS registers that connect to application servers located at each store. These registers use wired equivalent protection (WEP) encryption.
- **POS local application server locations**—The POS application server, usually located in the middle of each store's customer service area, forwards all sales data over a frame relay network to database servers located at the retailer's corporate headquarters, with strong encryption applied to the data, which are then sent over a virtual private network (VPN) to the credit card processor for approval of the sale.
- **Corporate database locations**—Corporate databases are located on a protected screened subset of the corporate local area network.
- **Sales data distribution**—Weekly aggregated sales data, by product line, are copied as-is from the corporate databases to magnetic media and mailed to a third party for analysis of buying patterns.
- **Current ERP system compliance**—The current state of the company's ERP system is such that it may be out of compliance with newer laws and

regulations. During the initial assessment, the IS auditor determined that the ERP system does not adhere to the EU's General Data Protection Regulation (GDPR).

Additionally, Wonderwheels' database software has not been patched in over two years, due to a few factors:

- The vendor's support for the database package was dropped due to it being acquired by a competitor and refocusing the remaining business to other software services.
- Wonderwheels' management has implemented plans to upgrade to a new database package. The upgrade is underway; however, it is taking longer than anticipated.

Regarding the database upgrade, sizeable customizations were anticipated and are being carried out with a phased approach of partial deliverables. These deliverables are released to users for pilot usage on real data and actual projects. Concurrently, design and programming of the next phase are ongoing. In spite of positive initial test results, the internal audit group has voiced that it has not been included in key compliance decisions regarding the configuration and testing of the new system. In addition, operational transactions are often queued, or "hang" during execution, and more and more frequently, data are corrupted in the database. Additional problems have shown up—errors already corrected have started occurring again and functional modifications already tested tend to present other errors. The project, already late, is now in a critical situation.

1. Which of the following would present the **MOST** significant risk to the retailer?
   A. Database patches are severely out of date.
   B. Wireless POS registers use WEP encryption.
   C. Credit cardholder information is sent over the Internet.
   D. Aggregate sales data are mailed to a third party.

2. Based on the case study, which of the following controls would be the **MOST** important to implement?

A. POS registers should use two-factor authentication, with enforced complex passwords.
B. Wireless access points should use MAC address filtering.
C. The current ERP system should be patched for compliance with GDPR.
D. Aggregate sales data should be anonymized and encrypted prior to distribution.

3. In the preliminary report to management, regarding the state of the database upgrade, which of the following is **MOST** important for the IS auditor to include?
A. Internal audit should be included among the steering committee approvals.
B. There is a possibility that the new database may not be compatible with the existing ERP solution.
C. An ERP upgrade and/or patch is required in order to ensure updated database compatibility.
D. Internal audit should be able to review the upgraded database to ensure compliance with Payment Card Industry Data Security Standard (PCI-DSS).

4. In order to contribute more directly to help address the problems around the database upgrade, the IS auditor should:
A. Review the validity of the functional project specifications as the basis for an improved software baselining definition.
B. Propose to be included in the project team as a consultant for QC of deliverables.
C. Research the problems further to identify root causes and define appropriate countermeasures.
D. Contact the project leader and discuss the project plans and recommend redefining the delivery schedule using the PERT methodology.

ANSWERS TO CASE STUDY QUESTIONS

1. A. Unpatched database servers are located on a screened subnet; this would mitigate the risk to the organization.

   B. Use of WEP encryption would present the most significant risk because WEP uses a fixed secret key that is easy to break. Transmission of credit cardholder information by wireless registers would be susceptible to interception and would present a very serious risk.

   C. Sending credit cardholder data over the Internet would be less of a risk because strong encryption is being used.

   D. Because the sales data being sent to the third party are aggregate data, no cardholder information should be included.

2. A. According to the case study, it is unclear whether or not the POS registers already use two-factor authentication. It is known that aggregate sales data are copied onto other media as-is, without any controls, for external distribution.

   B. According to the case study, it is unclear whether or not the wireless access points use MAC address filtering. It is known that aggregate sales data are copied onto other media as-is, without any controls, for external distribution.

   C. Compliance with the GDPR, while important, is not the most important due to the current operations being only in the US, and the potential for expansion into the EU is a long-term vision for the company.

   D. It is unclear whether or not sales data are secure and free of personally identifiable information, such as credit card information and Social Security numbers. This would present the most significant risk and should be addressed.

3. **A. If internal audit is part of the steering committee, then it will have a say in the compliance and security-related controls to be included in production releases.**

   B. Ensuring database compliance is an operational responsibility and not an audit responsibility.

   C. Compatibility with existing architecture must be a function of the database implementation project team as a whole, which can

include internal audit and also includes operations. Therefore, it is not the best choice.

D. While it is important that the upgraded database solution be compliant with all regulations affecting the company, such a review should not be limited to one regulation. Therefore, it is not the best choice of those provided.

4. A. Functional project specifications should be executed by users and systems analysts, and not by the auditor.

B. To propose to be project consultant for quality would not bring about an essential contribution since quality is a formal characteristic, whereas in the current case, the problem is a substantial system instability.

C. The only appropriate action is additional research, even if the apparently technical nature of the problem renders it unlikely that the auditor may find it alone.

D. To contact the project leader and redesign the schedule of deliveries would not solve the problem. Furthermore, the definition of real causes may sensibly alter the project environm