**BINS 4331**

**Fall 2022 Individual Project**

# \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Write a report to address all parts of the questions. Do not provide briefanswers to each question. Your answers should be in a report format. Use the risk assessment template provided to conduct risk analysis and submit a word document report with your name. You will lose 20 points if your answer is notin a report format, including the risk assessment template**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Read the following articles

1. PCI DSS Report
2. PCI DSS Breach Examples
3. PCI DSS Explained

Due to COVID-19 and consequent restrictions, the Girl's Guide (GG) cookies sale drive is planning to use only electronic payment, including credit cards for payments. The Girl's Guide Board of Directors has directed the IT Department to implement Payment Card Industry Data Security Standards (PCI DSS) before the organization begins accepting credit card payments

The IT Department currently manages a Wi-Fi Network, a wired network, and web servers that provide information to customers and clients, but the Department has no explicit security policies or controls. The only policy that it has implemented successfully is a password length and change policy which requires all users to use a 12-character length password and also change passwords every 6 months.

The strategy of the IT Department is to focus on 4 PCI DSS requirements listed in the **WorseAreas in PCI DSS Non-compliance** table from the Verizon 2020 Payment Security Report. As head of the IT Departments, you must perform a risk assessment and present a report to the BOD to justify the Department's selection and what strategies and tactics the Department will use to ensure compliance with the 4 PCI DSS requirements

|  |  |
| --- | --- |
| **\*Worst Areas of PCI Non-Compliance** | |
| **PCI Requirements** | **Non-Compliance Rate** |
| 1.Security Systems Processes and Testing | 48.1% |
| 2.Security Policies and Management | 45.5% |
| 3.Develop and Maintain Secure Systems | 39.6% |
| 4.Do Not Use Vendor Defaults | 35.1% |
| 5.Track and Monitor Access | 33.8% |
| 6.Install and Maintain Firewall | 31.2% |
| \*Data Source: Verizon 2020 Payment Security Report | |

Using the risk assessment template (RAT) provided, perform a risk assessment of the 4 areas that the IT Department selected. **An example of a completed template using UALR Student Records is provided for illustration as part of the project**.

In your assessment, evaluate the vulnerability assessment scale, threat impact scale, risk likelihood scale and assign appropriate values and compute the composite scale.

1. List the 4 PCI DSS requirements (after reviewing all three readings) What are the 4 PCI DSS requirement selected by the IT Department **(10 pts)**

The IT department has provided a mechanism to ensure that vendor defaults are not used in managing passwords used on the payment management system. The IT department is to build on the system's security by directing efforts to comply with other PCI DSS requirements. The IT department is to comply with the requirement of Security Systems Processes and Testing. This is followed up by the IT department working to ensure that the systems are developed to be secure and maintained. With the system being developed to help the organization handle different types of transactions, the requirement of tracking and monitoring access will be important. The installation and maintenance of a firewall are of utmost importance to control traffic through the established network.

1. Explain why the selected areas are important to PCI DSS implementation (**10 pts)**

The IT department has identified four PCI DSS requirements that it will endeavor to deliver. The IT department is to ensure that system processes are secure and tested. This will ensure that the systems are rid of inconsistencies. The interest in building and maintaining secure systems is with respect to implementing strong access control measures. The requirement of tracking and monitoring access will be taken on to checkthe security of network resources and cardholders' data. The installation and maintenance of a firewall are informed to help the organization build and maintain a secure network.

1. Using the Template Perform a risk assessment of the 4 PCI DSS requirements using the scales provided in Tables 1-4. **(10 pts)**

Please see table 1-4

1. Based on your risk assessment, write a brief report on your findings. As IT Department manager explains and briefly elaborate on how the IT Department evaluated and ascertained the impact scale for threats, vulnerability, and risks. Justify your values **(20 pts)**

The organization intends to interact with external stakeholders that will be customers of the cookies on sale. The systems being used to facilitate the transactions need to be reliable to seamlessly help the organization provide customers with a convenient payment method. At the same time, they maintain that their data is securely maintained. Therefore, the systems' processes need to be effective while maintaining acceptable security standards. This, therefore, necessitates that the network being used be maintained to be secure from vulnerabilities that may be exploited to deter the organization's desired efficacy as it conducts business and strives to secure cardholders' data.

1. In your report as IT Department Manager, explain the composite score to the Girl's Guide BOD and explain the strategy of the IT department given the Composite Score Level for the 4 PCI DD Requirements. **(20 pts)**

Given the systems' critical need for the maintenance of cardholders' data security and being exceptional in the handling of the transactions being conducted, the core risk scores for the requirements of Security Systems Processes and Testing, Track and Monitor Access, and Install and Maintain Firewall were in the range of 7 to 9. The requirement of Develop and Maintain Secure Systems composite risk score was 5. The requirements measured to be high according to the Composite Score Level will have the IT department develop strategies that will be implemented and reviewed regularly throughout the year. The requirement of Develop and Maintain Secure Systems Composite Score Level is medium, and reviews are to be conducted yearly. The accompanying concepts encompassed by the selected PCI DSS requirements will inform each strategy to be implemented and reviewed.

1. As head of the IT Department, use the report to explain specific processes/policies in the tactical plans of the IT Department to comply with those selected PCI areas. These plans should include specific IT controls/processes to support compliance with the 4 PCI DSS requirements **(30 points)**

The organization is to take up the use of compliance requirements for the implementation of the selected PCI DSS requirements. The compliance requirements to be used for the organization's benefit include the utilization of a Self-Assessment questionnaire, Vulnerability scan, and attestation of compliance. The vulnerability scan is to be employed for each selected PCI DSS requirement with respect to the recommendations evaluated best for them according to the attained Composite Score Level. The results of the vulnerability scans are to inform the application of the self-assessment questionnaire. Actions taken to post to the undertaken measures are to be conducted to get the organization to comply with the provisions articulated for the PCI DSS requirements selected.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**….3….**Using the Template Perform a risk assessment of the 4 PCI DSS requirements using the scales provided in Tables 1-4. **(10 pts)**

## PCI DSS Risk Assessment Template

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Selected PCI DSS**  **Requirements from**  **Worst Areas of Non-**  **Compliance** | **Threat Impact Scale** | | | **Vulnerability**  **Assessment**  **Scale** | | | **Risk**  **Likelihood**  **Scale** | | | **Composite Risk Score and Level** | |
| L | M | H | L | M | H | L | M | H | **Score** | **Level** |
| 1.Security Systems Processes and Testing |  | 2 |  |  |  | 3 |  | 2 |  | 7 | H |
| 3.Develop and Maintain Secure Systems |  | 2 |  |  | 2 |  | 1 |  |  | 5 | M |
| 5.Track and Monitor Access |  |  | 3 |  | 2 |  |  | 2 |  | 7 | H |
| 6.Install and Maintain Firewall |  |  | 3 |  |  | 3 |  |  | 3 | 9 | H |

|  |  |  |
| --- | --- | --- |
| **Table 1: Vulnerability Assessment Scale** | | |
| Levels | | Explanation |
| H | 3 | Exploited vulnerability impacts organization |
| M | 2 | Exploited vulnerability impacts functional units |
| L | 1 | Exploited vulnerability impact is minor |

|  |  |  |
| --- | --- | --- |
|  | | **Table 2: Risk Likelihood Scale** |
| Levels | | Explanation |
| H | 3 | High probability that risk will occur |
| M | 2 | Medium probability that risk will occur |
| L | 1 | Low probability that risk will occur |

|  |  |  |
| --- | --- | --- |
|  | | **Table 3: Threat Impact Scale** |
| Levels | | Explanation |
| H | 3 | Threat potential impacts organization |
| M | 2 | Threat potential impact limited to functional units |
| L | 1 | Threat potential is limited and minor |

|  |  |  |
| --- | --- | --- |
|  | **Table 4: Composite Score Scale** | |
| **Level** | **Composite Risk Score** | **Recommended Annual Review** |
| H | 7-9 | Monitor risk regularly during the year |
| M | 4-6 | Monitor risk yearly |
| L | 1-3 | Regularly Monitor risk during a 2–3year period |