**Project X**

# DETAILED RISK ASSESSMENT REPORT

## Executive Summary

Very brief summary your findings

# DETAILED ASSESSMENT 1. Introduction

## 1.1 Purpose

The purpose of the risk assessment was to identify threats and vulnerabilities related to …….

## 1.2. Scope of this risk assessment

Describe the website components and architecture being used. (for example: Including things like how payments are made)

# 2. Risk Assessment Approach

## 2.1 Participants

|  |  |
| --- | --- |
| **Role** | **Participant** |
| System Owner | You may not have all these rolls |
| System Custodian |  |
| Security Administrator |  |
| Database Administrator |  |
| Network Manager |  |
| Risk Assessment Team |  |

## 2.2 Techniques Used

|  |  |
| --- | --- |
| **Technique** | **Description** |
| Risk assessment questionnaire | I would use here the documents from the notes when we talked about. The standards for security. |
| Assessment Tools | If you used any…. |
| Vulnerability sources | The team accessed several vulnerability sources to help identify potential vulnerabilities. The sources consulted included……..: |

|  |  |
| --- | --- |
| **Technique** | **Description** |
| Transaction walkthrough |  |
| Review of documentation |  |
| Interviews |  |
| Site visit |  |

## 2.3 Risk Model

In determining risks associated with Project X, we utilized the following model for classifying risk:

*Risk = Threat Likelihood x Magnitude of Impact*

And the following definitions:

**Threat Likelihood**

|  |  |
| --- | --- |
| **Likelihood (Weight Factor)** | **Definition** |
| High (1.0) | The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective |
| Medium (0.5) | The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. |
| Low (0.1) | The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. |

**Magnitude of Impact**

|  |  |
| --- | --- |
| **Impact (Score)** | **Definition** |
| High (100)    Replace these | The loss of confidentiality, integrity, or availability could be expected to have a *severe or catastrophic* adverse effect on organizational operations, organizational assets, or individuals.    Examples:   * *A severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions* * *Major damage to organizational assets* * *Major financial loss* * *Severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.* |
| Medium (50)      And these | The loss of confidentiality, integrity, or availability could be expected to have a *serious* adverse effect on organizational operations, organizational assets, or individuals.   * *Significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced* * *Significant damage to organizational assets* * *Significant financial loss* * *Significant harm to individuals that does not involve loss of life or serious life threatening injuries.* |
| Low (10)    And these | The loss of confidentiality, integrity, or availability could be expected to have a *limited* adverse effect on organizational operations, organizational assets, or individuals.    Examples:     * *Degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced* * *Minor damage to organizational assets* * *Minor financial loss* * *Minor harm to individuals.* |

**Risk was calculated as follows:**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Impact** | |  |
| **Threat Likelihood** | *Low*  *(10)* | *Medium*  *(50)* | *High (100)* |
| High (1.0) | Low Risk (10 x 1.0 = 10) | Medium Risk  (50 x 1.0 = 50) | High Risk (100 x 1.0 = 100) |
| Medium (0.5) | Low Risk  (10 x 0.5 = 5) | Medium Risk  (50 x 0.5 = 25) | Medium Risk  (100 x 0.5 = 50) |
| Low (0.1) | Low Risk  (10 x 0.1 = 1) | Low Risk  (50 x 0.1 = 5) | Low Risk (100 x 0.1 = 10) |

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)

# 3. System Characterization

## 3.1 Technology components

|  |  |
| --- | --- |
| **Component Description** | |
| Applications |  |
| Databases |  |
| Operating Systems |  |
| Networks |  |
| Interconnections |  |
| Protocols | Some of these may not apply |

## 3.2 Physical Location(s)

|  |  |
| --- | --- |
| **Location** | **Description** |
| Data Center | 260 Somewhere Street, Anytown |
| Help Desk | 5500 Senate Road, Anytown |
| NOC (Network Operations Center) | 1600 Richmond Avenue, Anytown |

## 3.3 Data Used By System

|  |  |
| --- | --- |
| **Data Description** | |
| Personally identifiable information | Includes:   * Name * Address (current and previous) * Phone Number * SSN # * DOB |
| (as an example, you may not have this row)  Patient information | Includes       Same here, you’ll want something else, these are samples |
| Financial information | * *Credit card #* * *Verification code* * *Expiry date* * *Card type* * *Authorization reference* * *Transaction reference* |

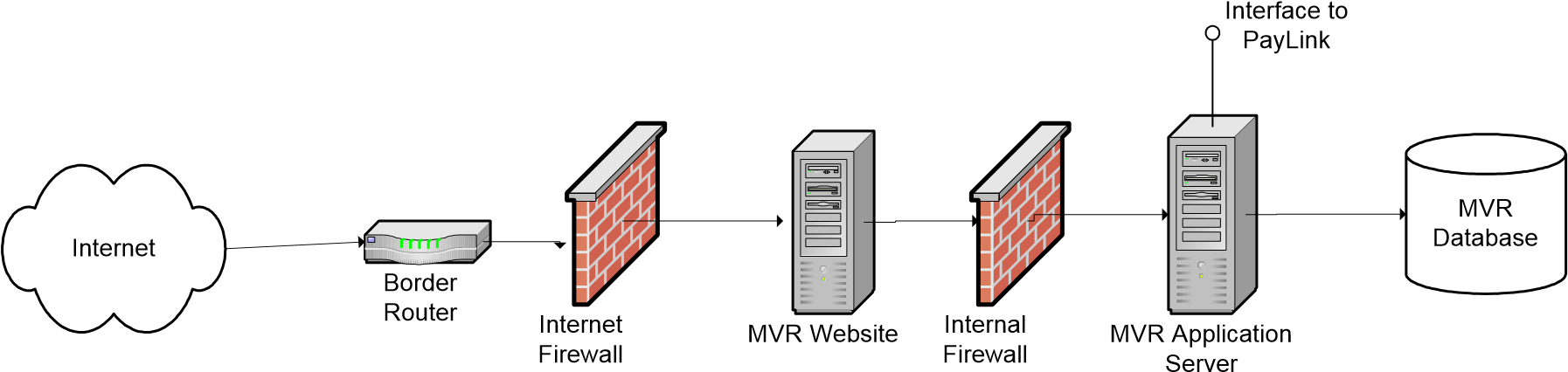
## 3.4 Users

|  |  |
| --- | --- |
| **Users** | **Description** |
|  |  |
|  |  |
|  |  |
|  |  |

## 3.5 Flow Diagram

The following diagram shows the in-scope technology components reviewed as part of the MVROS.

This is the example, yours may be close



# 4. Vulnerability Statement

The following potential vulnerabilities were identified:

|  |  |
| --- | --- |
| **Vulnerability Description** | |
| Cross-site scripting | I think you’ll all have these |
| SQL injection |  |
| Password strength |  |
| Unnecessary services |  |

|  |  |
| --- | --- |
| **Vulnerability** | **Description** |
| Disaster recovery |  |
| Lack of documentation |  |
| Integrity checks | The system does not perform sufficient integrity checks on data input into the system. |

# 5. Threat Statement

The team identified the following potential threat-sources and associated threat actions applicable to the XXXXXX:

|  |  |
| --- | --- |
| **Threat-Source** | **Threat Actions** |
| Hacker | Probably use these |
| Computer criminal |  |
| Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees) |  |
| Environment |  |

# 5. Risk Assessment Action Items

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Item**  **Number** | **Observation** | **Threat-Source/ Vulnerability** | **Existing controls** | **Likelihood** | **Impact** | **Risk Rating** | **Recommended controls** |
| 1 |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |

*This is sample data for demonstration and discussion purposes only*

Page 10

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Item**  **Number** | **Observation** | **Threat-Source/ Vulnerability** | **Existing controls** | **Likelihood** | **Impact** | **Risk Rating** | **Recommended controls** |
|  |  |  |  |  |  |  |  |

*This is sample data for demonstration and discussion purposes only*

Page 11