

**VULNERABILITY**

**ASSESSMENT AND PENETRATION TEST**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**{{ cover\_date }}**

**Description**

**This document details the process and results of a Vulnerability Assessment, Penetration Test**

**performed by Baker Tilly Digital on behalf of {{ case**.**organization }} between {{** **case.createDate }} and {{** **case**.**lastUpdate}}.**

**Prepared for {{ case.organization }}**

{{ case.logo }}

**Author**

**Baker Tilly Digital**

[**digital@bakertilly.co.zw**](mailto:teamdigital@bakertilly.co.zw)

# Document control

DOCUMENT PROPERTIES

|  |  |
| --- | --- |
| **Property** | **Value** |
| Client | **{{ case**.**organization }}** |
| Client contact | **{{ case**.**orgHandler }}** |
| Document title | IT Audit and Security Assessment |
| Document classification | PRIVATE AND CONFIDENTIAL |
| Author(s) | Baker Tilly Digital |
| Manager | {{ case.caseLead }} |
| Date | {{ date }} |

DISTRIBUTION LIST

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Reason** |
| **{{ case**.**orgHandler }}** |  |  |
|  |  |  |

VERSION CONTROL

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Author(s)** | **Comment** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Vulnerability Assessment & Penetration Test (VAPT) Report**

For {{ case.organization }}

**PRIVATE & CONFIDENTIAL**

**NON-DISCLOSURE STATEMENT & LEGAL NOTICE**

All information obtained during this cyber security assessment about {{ case.organization }}'s systems and assets including (but not limited to) its procedures and systems, is deemed privileged information and not for public dissemination. Baker Tilly staff severally pledge their commitment that this information will remain strictly confidential. This information will not be disclosed or discussed to any third party without the express written consent of {{ case.organization }}. Baker Tilly is fully committed to maintaining the highest level of ethical standards in its business practice.

# 

# HOW TO USE THIS REPORT

**Executive Summary**

The Executive summary highlights the main findings from the report and provides an indication as to the level of controls and security of {{ case.organization }}’s target environment.

**Summary of Findings**

This section shows a summary of the issues found on each target accompanied by a bar chart to demonstrate the number of vulnerabilities found on each target and their severity.

The vulnerabilities are counted by their type and not instances of the same vulnerability. For example, Cross Site Scripting is classified as a single vulnerability even though multiple pages may have the same issue.

**Detailed Technical Report**

This section lists the detailed findings found for each target and contains the low to serious vulnerabilities. Each vulnerability includes an indication of its **Impact**, a description, results and how it can be resolved. Whenever possible, an exploit for the identified vulnerability will be supplied.

**Section:**

**Internal VAPT**

This section goes in-depth with regards to the process followed and results obtained in carrying out the internal VAPT onsite at {{ case.organization }} premises. The section also

**External VAPT**

This section goes in-depth with regards to the process followed and results obtained in carrying out the external VAPT onsite at {{ case.organization }} publicly accessible digital assets.

**Subsection:**

**Penetration Test**

These are in-depth/technical results of the penetration tests conducted on behalf of {{ case.organization }}. The Baker Tilly Digital Team was able to exploit several vulnerabilities found on {{ case.organization }}’s digital assets. It is to be noted that these results are as at a particular point in time with the prevailing environmental variables in place.

**Vulnerability Assessment**

The Baker Tilly Digital team carried out both manual and automated vulnerability assessment. This section provides insight into occurrence, severity and recommendations for the vulnerabilities discovered during the assessment.

**Table of Contents**

[Document control ii](#_Toc109267139)

[HOW TO USE THIS REPORT v](#_Toc109267140)

[2 EXECUTIVE SUMMARY 8](#_Toc109267141)

[**2.1** Overview 8](#_Toc109267142)

[**2.2** Scope of work 8](#_Toc109267143)

[**2.3** Testing overview 8](#_Toc109267145)

[**2.4** Our approach 9](#_Toc109267146)

# EXECUTIVE SUMMARY

# 

## Overview

{{ case.organization }} engaged Baker Tilly Digital to conduct a Vulnerability Assessment and Penetration Test of its IT infrastructure and internal network as well as the external network from {{ case.createDate }} to {{ case.lastUpdate }}.

{{ issues\_count }} critical vulnerabilities were identified which could compromise the confidentiality, availability, and integrity of the servers, and potentially create a foothold for further penetration into the enterprise.

The goal of this engagement was to conduct targeted testing and controls audit to ensure broad coverage of the most common types of vulnerabilities as defined by the OWASP (Open Web Application Security Project) Top 10 and general IT controls. The assessment also did not perform any denial of service (DoS) attacks against the network, its subsystems, devices or applications in order to minimize the potential of interrupting operations.

## Scope of work

## 

IP Addresses



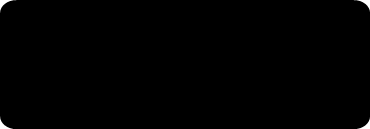


Figure 1: Scope of work

## Testing overview

{{ case.lastUpdate }}

•

Discover vulnerabilities

•Non-Destructive exploitation

Objective

•

{{ case.createDate }}

•

Time Span

•

{{ case.assessmentType }} Testing

Methodology

Figure 2: Testing overview

## Our approach

Scope of Work &

Information

Gathering

Identify Active Machines

And Fingerprinting

Target Hosts

Scan And

Enumerate

Services

Identify

Attack

Surface

Automated and Manual

Vulnerability

Assessments

Exploit

Vulnerabilities

Identify

Impact

Provide

Recommendations

Report

Figure 3 :Baker Tilly Pentest Approach

# Standards and Frameworks followed.

1. Pentest standards [www.pentest](http://www.pentest)[-](http://www.pentest-standard.org/)standard.org
2. Open Web Application Security Testing Framework (OWASP)
3. Web Application Security Consortium (WASC)
4. The Open Source Security Testing Methodology Manual (OSSTMM)
5. National Institute of Standards and Technology (NIST) which one
6. National Vulnerabilities Database (NVD)

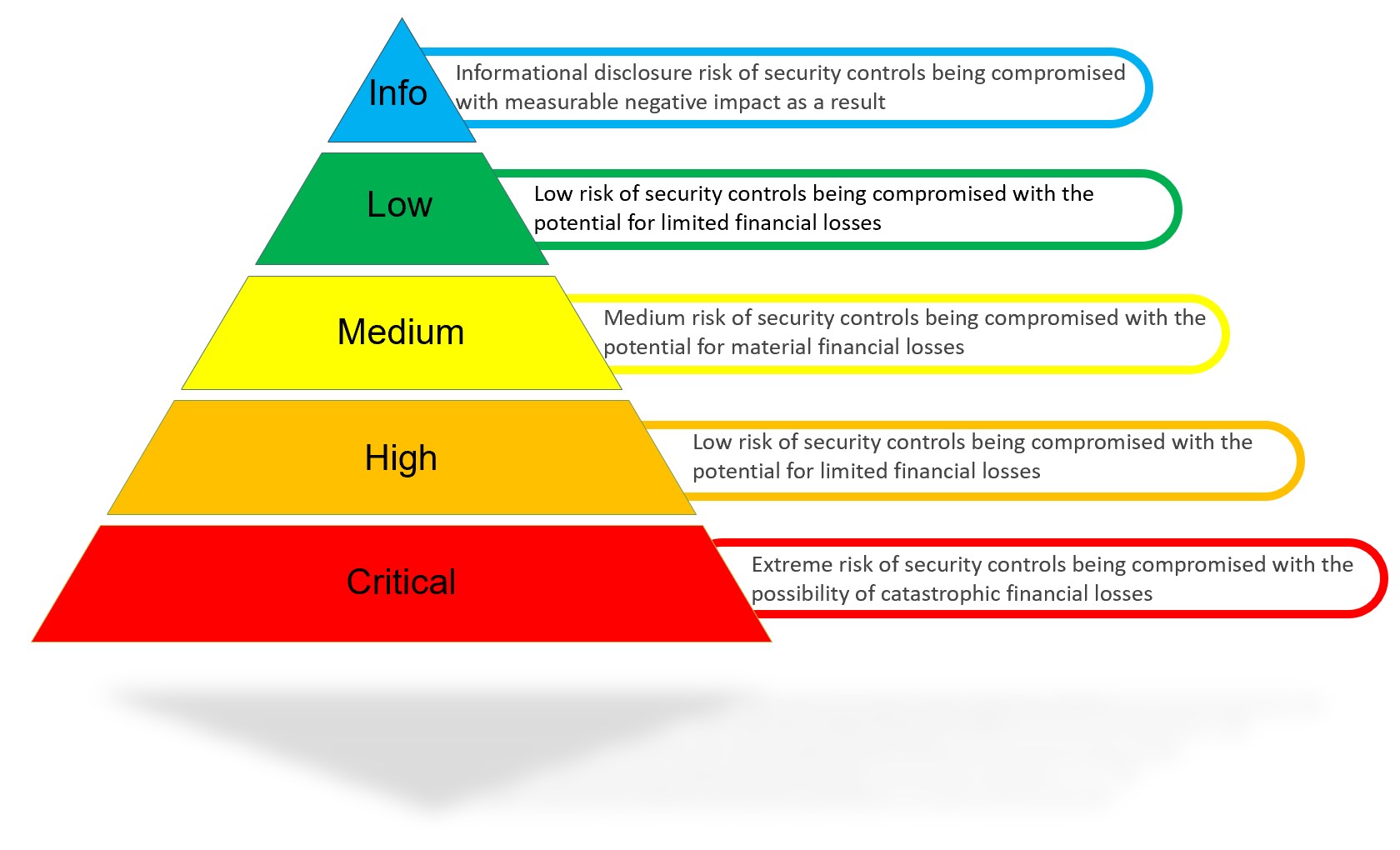
# Severity ratings

Baker Tilly follows the Common Vulnerability Scoring System (CVSS) scoring system to rate vulnerabilities.

The CVSS assessment measures three areas of concern:

1. **Base Metrics** for qualities intrinsic to a vulnerability
2. **Temporal Metrics** for characteristics that evolve over the lifetime of vulnerability
3. **Environmental** Metrics for vulnerabilities that depend on an implementation or environment

For more information on what the Base, Temporal, and Environment Metrics in the CVSS scoring system are, for more information please refer to <https://www.first.org/cvss/specification-document>



*Figure 4: Vulnerabilities* ***Impact*** *score*

|  |  |
| --- | --- |
| **CVSS Severity Rating** | **CVSS Score** |
| **Critical** | 9.0 - 10.0 |
| **High** | 7.0 - 8.9 |
| **Medium** | 4.0 - 6.9 |
| **Low** | 0.1 - 3.9 |
| **None / Informational** | 0.0 |

# Summary of findings

## Vulnerability by severity

Below is the table that summarizes the list of findings discovered during the assignment:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Title** | **Affected** | **Severity** | **Impact To Business** | **CVSS Rating** | **Key Remediation** |
| {%tr for issue in issues %} | | | | | |
| {{ issue.name }} | *{{ issue.affected\_hosts }}* | {% if issue.severity == “Critical” %} **{{ issue.severity }}**  {% elif issue.severity == “High” %}  **{{ issue.severity }}**  {% elif issue.severity == “Medium” %}  **{{ issue.severity }}**  {% elif issue.severity == “Low” %}  **{{ issue.severity }}**  {% elif issue.severity == “Info” %}  **{{ issue.severity }}**  {% endif %} | {{ issue.impact }} | {% if issue.cvss\_rating and issue.cvss\_rating >= 9 %} {{ issue.cvss\_rating }}  {% elif issue.cvss\_rating and issue.cvss\_rating >= 7 %}  {{ issue.cvss\_rating }}  {% elif issue.cvss\_rating and issue.cvss\_rating >= 4 %}  {{ issue.cvss\_rating }}  {% elif issue.cvss\_rating and issue.cvss\_rating >= 0.1 %}  {{ issue.cvss\_rating }}  {% elif issue.cvss\_rating and issue.cvss\_rating == 0 %}  {{ issue.cvss\_rating }}  {% endif %} | {{ issue.solution }} |
| {%tr endfor %} | | | | | |

Table 1: Vulnerability summary

# EXTERNAL VAPT

{% for issue in issues %}

**Host(s) affected:** {{ issue.affected\_hosts }}

**Issue:** {{ issue.name }}

**Risk Description**

{{ issue.description }}.

**Impact**

{{ issue.impact }}

{% if issue.poc\_list %}

**Proof of Concept**

{% for poc in issue.poc\_list %}

{{ poc }}

{% endfor %}

{% endif %}

{% endfor %}