AUDIT REPORT – IT DEPARTMENT

<COMPANY HIDDEN>

OZONE EXCELLENCE CONSULTING

TEL: (971) 4 354 3440 Web: www.oz1consulting.com Email: ozone@oz1consulting.com

Table of Contents

EXECUTIVE SUMMARY:

OEC would like to thank the management at <COMPANY HIDDEN> for the opportunity to audit and report on the infrastructure and processes within the IT department at <COMPANY HIDDEN>.

We conclude that the IT Department at <COMPANY HIDDEN> "Needs Improvement". This indicates that that a combination of weaknesses in the system of control and minor non-compliances with the controls in place is such as to place service objectives at risk.

We have identified **5 High Impact; 3 Medium Impact; and 3 Low Impact** Opportunities for <COMPANY HIDDEN> Management to consider. We have summarized these opportunities on Page 20 of this report.

Our report is structured as follows.

- In the first section titled "Current State of IT Infrastructure at <COMPANY HIDDEN>" we have provided our observations related to the procedures and the equipment being used at <COMPANY HIDDEN>. This section allowed us to set a baseline for the department.

- In the next section "Future State of IT infrastructure at <COMPANY HIDDEN>" we describe the characteristics of an ideal IT setup. We further describe the primary areas pertinent to each subsection that are in need of improvement.

- In the section "Findings and Recommendations" we provide a detailed list of improvement projects with a commentary on the risks associated with non-compliance. Additionally we provide a recommended action plan for the management to consider with a budgetary figure (wherever applicable).

Our Top 3 Positives for the IT Department are as follows:

- XXXX
- XXXX
- XXXX

Our Top 3 areas of Improvement for the IT department are as follows:

- XXXX
- XXXX
- XXXX

1.0 INTRODUCTION:

1.1 Objective

This third party audit includes review of the IT Infrastructure assets, business processes and practices at <COMPANY HIDDEN>, located in <PLACE HIDDEN>. The purpose of the audit is to provide an independent and objective assurance on the existing risks and controls in the IT Department at <COMPANY HIDDEN>. This review will focus on assessing whether internal controls are adequately designed and are operating effectively to address risks.

This report presents the audit findings with observations and best practice recommendations where there may be opportunities for improvement.

1.2 Background

XXXX

1.3 Scope of Engagement

The scope of the engagement is to conduct an audit assessment of the following aspects of the IT Department at <COMPANY HIDDEN>, which includes:

- Evaluate the metrics and mandate provided to the IT Department by the Management at <COMPANY HIDDEN>.
- Review of assets within the IT Department.
- Review of warranties (as applicable) and responsibilities for maintenance.
- Review of specialized contractors for outsourced works scope including their job completion reports.
- Visual inspection of assets (wherever applicable) to check for abnormalities, discrepancies, gaps and integrity.
- Review of Operational Procedures/SLA/Manuals.
- Review content and understanding of SOP's, Manuals and their adherence thereof.
- Review current manpower levels within the department.
- Identify the equipment that has not been maintained properly and costing of remedial works to put back to standard.
- Review report generation, trending and system performance and their accuracy thereof.
- Provide recommendations for all of the above mentioned areas.

1.4 Approach for Engagement

The approach of the engagement is as follows:

- A detailed understanding of the processes was obtained by interviewing the Process owners based on comprehensive checklist covering the processes and sub process of the IT Department.

- Copies of system documents were requested and reviewed to familiarize and understand the completeness of the departmental processes. Multiple site visits were also undertaken to review the performance of the department and infrastructure.

- Key risks and controls were identified and documented based on process understanding, site surveys and interviews conducted.

- Detailed examination of key documents related to the process and sub processes was conducted based on the identified risks.

- The observations and recommendations in this report are based upon reviewing the documents and infrastructure, doing site inspections, auditors' previous experience in IT audits, best practices and benchmarks in IT Department including documentation provided by <COMPANY HIDDEN> personnel and discussions with the Process Owners and Senior Management.

1.5 Acknowledgement

We would like to take this opportunity to thank the management and staff at<COMPANY HIDDEN>for their cooperation and assistance during the course of the engagement. We are committed to offering you excellent service and look forward to building a long and value-added relationship with you.

1.6 Limitation

This third party audit procedures rely on information and representations made available to the auditors by the process owners and key individuals associated with the processes. Our third party audit procedures comprise inquiries, observations and limited tests of transactions on a sample basis, covering the detailed assessment objectives.

Any misrepresentation intentional or otherwise may affect the results and recommendations of this audit.

2.0 CURRENT STATE OF THE IT INFRASTRUCTURE AT <COMPANY HIDDEN>:

2.1 Policies and Procedures

Topic	**2.1.1 Mission Statement for IT Department**
Key Points	2.1.1.1 OEC did not find a documented mission statement for the IT department. 2.1.1.2 XXXX

Topic	**2.1.2 XXXX**
Key Points	2.1.2.1 OEC did not find any XXXX 2.1.2.2 For servers' administrator credentials: OEC found XXXX 2.1.2.3 For user machines' administrator credentials: OEC found that XXXX. XXXX 2.1.2.2 OEC was provided XXXX. We feel this form is inadequate for the organization. We were provided with a sample hard copy of this Entry form. (Appendix 1). 2.1.2.3 OEC was provided with a sample hard copy of the XXXX. (Appendix 2). 2.1.2.4 OEC notes that the IT department works on multiple verbal and informal processes. However it is highly recommended that XXXX

Topic	**2.1.3 Licensing**
Key Points	2.1.3.1 OEC auditors found that the licensing details XXXX 2.1.3.2XXXX

Topic	**2.1.4 Procurement**
Key Points	2.1.4.1 Our auditors noted that new hardware requisitions are directed to the IT team first for approval. The newly procured asset details with the asset name, Employee code, name of the assigned person, department name, specifications are saved in an asset tracker by the IT team. We were provided with the sample copy of the same. (Appendix 4).

	2.1.4.2 We noted that printers are being leased. (A license agreement copy was provided for our records. (Appendix 5). 2.1.4.1 We noted that the IT team is responsible for the procurement of servers, network devices, storage devices based on the design needs from the IT department. 2.1.4.2 **Software and Hardware:** We could see that the new software and hardware requisitions are directed to the IT team by the IT department leads through mail. Purchase of mouse and keyboard do not need any approval. External hard disks are provided for some specific departments. 2.1.4.3 OEC noted that XXXX

2.2 Server Level Infrastructure

Topic	**2.2.1 Servers**
Key Points	2.2.1.1 We found the following servers in the data center. Configurations of these servers are noted below: • XXXX • XXXX • XXXX
	2.2.1.2. OEC found that the cluster server hosts eight (8) Virtual machines (VMs) that serve the following functionalities: • XXXX The virtual machines are based on the XXXX technology provided by XXXX. (Appendix 13)

Topic	**2.2.2 Storage Devices**
Key Points	2.2.2.1 We noted the following storage devices in the <COMPANY HIDDEN> environment. Specifications are as below: **Storage Device 1:** • XXXX

	Storage Device 2: • XXXX

Topic	2.2.3 Virtualization Technologies
Key Points	2.2.3.1 OEC auditors noted that the IT department at <COMPANY HIDDEN> uses XXXX 2.2.3.2 XXXX 2.2.3.3 XXXX 2.2.3.4 XXXX

2.3 Server Applications

Topic	2.3.1 Email System Management
Key Points	2.3.1.1 OEC auditor's observations are noted below: • <COMPANY HIDDEN> uses MS Exchange 2013 for email service. • XXXX • XXXX • The IT team currently manages 124 mailboxes. • The maximum size of user's mailbox is restricted to 5 GB. • The maximum size of the mailbox for management team is 20 GB per user. • The IT department advises users to archive their individual mailboxes once they reach their stipulated mailbox limits. • Both the IT team and the user store the archive copy of the individual mail boxes. IT team stores it on an external hard disk (IT hard disk) while the user saves it on his/her local machine. • XXXX • The IT team did not XXXX

Topic	2.3.2 Active Directory
Key Points	2.3.2.1 We found that there is one domain used across the company. It is named "<Company Hidden>.local". It hosts 65 domain users. 2.3.2.2 We noted that the version of AD is the default provided by the XXXX 2.3.2.3 XXXX 2.3.2.4 We could not find a XXXX

Topic	2.3.3 ERP
Key Points	2.3.3.1 <COMPANY HIDDEN> uses XXXX ERP system as its primary data management system. 2.3.3.2 The ERP application is hosted on: • A frontend application server (Virtual Machine) with an allocated RAM of 16GB. The server name is XXXX • A backend SQL Server (Virtual Machine) with an allocated RAM of 16GB. The server name is XXXX 2.3.3.3 XXXX ERP uses sign-on credentials that are separate than Active Directory. The user credentials are maintained by IT team in two locations: on the application server and on the external IT hard disk. 2.3.3.4 The total size of data hosted on XXXX is about XXXX 2.3.3.5 XXXX 2.3.3.6 The vendor provides an AMC for the system. This AMC includes updates and patches for the ERP. (Appendix 7) 2.3.3.7 XXXX 2.3.3.8 We could not find any XXXX

Topic	2.3.4 HR Application
Key Points	2.3.4.1 The IT department hosts a separate HR application (legacy software) developed in-house. 2.3.4.2 XXXX 2.3.4.3 XXXX

Topic	2.3.5 Time Application
Key Points	2.3.5.1 The IT Department hosts a separate Time Management Application named XXXX software (very old software). 2.3.5.2 XXXX 2.3.5.3 XXXX 2.3.5.4 XXXX

Topic	2.3.6 Backup Policy
Key Points	2.3.6.1 <COMPANY HIDDEN> uses XXXX as its backup software. 2.3.6.2 XXXX is used for backup of physical servers as well as virtual machines. 2.3.6.3 XXXX currently possess the following backup licenses: • XXXX • XXXX 2.3.6.4 We were provided with a copy of the backup schedule for the virtual machines (Appendix 8). 2.3.6.5 All Virtual Machines are backed-up separately through XXXX. <COMPANY HIDDEN> currently maintains the following backup schedule (based on the document provided): • A full backup is scheduled to run biweekly on a single virtual machine on a certain day of the week. This is normally scheduled for either 7PM or 9PM. • Incremental backup is scheduled to run everyday for the following servers: - XXXX - XXXX • Incremental backup is scheduled to run on a particular day, once a week for the following servers: - XXXX - XXXX - XXXX - XXXX 2.3.6.6 OEC auditors found the following information regarding backup of User PCs: • XXXX • XXXX 2.3.6.7 A physical machine is used as the backup server. OEC noted that this machine is outdated and should be upgraded to current standards. 2.3.6.8 XXXX 2.3.6.9 A storage device is connected to the backup server. OEC was unable to obtain any details regarding the configuration of this device. 2.3.6.10 XXXX 2.3.6.11 OEC found that there is no XXXX

	2.3.6.12 We did not find any documented procedures for backup or restore processes within the IT department.

2.4 Security & Network Devices

Topic	**2.4.1 Firewall**
Key Points	2.4.1.1 We found that currently one Firewall is used in the <COMPANY HIDDEN> environment. It is a XXXX 2.4.1.2 OEC found an absence of an accurate network topology diagram in <COMPANY HIDDEN>. OEC has illustrated the network topology diagram as per our findings, in Appendix 12. 2.4.1.3 We observed that the IT Department provides VPN connectivity to its offsite clients using the 10 complimentary connections available through this device. 2.4.1.4 Currently we observed that around XXXX 2.4.1.5 User credentials for the VPN service are separate from those of Active Directory or the ERP Application. These are stored locally on the XXXX 2.4.1.6 We found that the IT department also maintains a record of the user credentials for the VPN accounts in a file. This also contains the mappings between the VPN account and the associated user. 2.4.1.7 We found that the passwords for these accounts are never changed.

Topic	**2.4.2 Switches**
Key Points	2.4.2.1 We found that <COMPANY HIDDEN> has a total of 5 switches in their environment. The model is XXXX 2.4.2.2 Of these five switches, 4 are used in the server room and 1 is used with the backup server. 2.4.2.3 Two switches have 48 ports while the other 3 have 24 ports.

Topic	**2.4.3 Wireless Access Points**
Key Points	2.4.3.1 <COMPANY HIDDEN> uses XXXX to provide the wireless access points across the facility.

	2.4.3.2 We observed 2 wireless access points: XXXX 2.4.3.3 <COMPANY HIDDEN> uses a Guest Wireless account for outsiders. XXXX. 2.4.3.4 We did not find XXXX to obtain wireless access. Also XXXX were also not found.

Topic	**2.4.4 User machine firewalls**
Key Points	2.4.4.1 OEC auditors observed that a XXXX is enabled on user machines. 2.4.4.2 We noted the following details regarding Windows updates: • For servers: XXXX • For user computers: XXXX 2.4.4.3 We could not find XXX within the department related to updates and patches.

Topic	**2.4.5 Antivirus/Malware**
Key Points	2.4.5.1 Our auditors noted that the antivirus software used at <COMPANY HIDDEN> is XXXX 2.4.5.2 The auditors were told that the XXXX was updated automatically. 2.4.5.3 We reviewed logs from the XXXX and could not find any XXXX within the system.

Topic	**2.4.6 Other Security software**
Key Points	2.4.6.1 We couldn't find any other security software installed in the system

Topic	**2.4.7 Internet Security Policies**
Key Points	2.4.7.1 Internet Restrictions – XXXX 2.4.7.2 Download Restrictions –XXXX 2.4.7.3 Personal Email Restrictions – XXXX

	2.4.7.4 External Device Restrictions – XXXX

2.5 User Level Infrastructure

Topic	**2.5.1 Desktops/Laptops**
Key Points	2.5.1.1 The <COMPANY HIDDEN> IT team noted that there were a total of 65 desktops/laptops with XXXX. These details are maintained in an XXXX. The auditors did not personally audit the presence of these workstations (Appendix 4). 2.5.1.2 OEC auditors were informed that the specifications for the user computers XXXX

Topic	**2.5.2 Tablets/Cell phones**
Key Points	2.5.2.1 The IT department has issued two tablets for use within the company. 2.5.2.2 We noted that <COMPANY HIDDEN> does not issue any handsets/phones to its employees. 2.5.2.3 OEC did find that the IT department issues SIM cards to employees on a 'as needed' basis. The SIM usage is monitored for 3 months and the package is adjusted accordingly. 2.5.2.4 OEC auditors were informed that the current count for <COMPANY HIDDEN> issued SIM cards is approximately XXXX (Appendix 9). 2.5.2.5 We were unable to find XXXX

Topic	**2.5.3 Computer Policies**
Key Points	2.5.3.1 We noted that any XXXX are communicated to the users verbally during their initial orientation. 2.5.3.2 We did not find any documentation regarding XXXX 2.5.3.3 We found anecdotal evidence that XXXX 2.5.3.4 XXXX

2.6 User Applications

Topic	2.6.1 Software and Licenses
Key Points	1.6.1.1 We found a document titled XXXX 1.6.1.2 XXXX 1.6.1.3 We did not find any XXXX

2.7 Remote Access

Topic	2.7.1 Remote Desktop Connectivity
Key Points	2.7.1.1 Our auditors noted that remote users connected through XXXX to the corporate network. 2.7.1.2 OEC found that XXXX is used to connect to the servers for maintenance/other tasks. 2.7.1.3 It was noted that there were no performance related issues reported.

2.8 SLA/Power Back Ups

Topic	2.8.1 XXXX
Key Points	2.8.1.1 XXXX 2.8.1.2 XXXX

2.9 Peripheral Services

Topic	2.9.2Printers/Scanners/Copiers
Key Points	2.9.2.1 We were informed that the printers are being leased 2.9.2.2 OEC was provided with a copy of the printer maintenance AMC (Appendix 5). 2.9.2.3 OEC concludes that this arrangement appears to be cost effective and adequate maintenance is provided.

	2.9.2.4 We could see some small printers used in XXXX department as these are located far from the main office. 2.9.2.5 Our auditors found that the XXXX 2.9.2.6 OEC was informed that a XXXX

3.0 PROPOSED STATE FOR THE IT INFRASTRUCTURE AT <COMPANY HIDDEN>:

Information technology (IT) has become a vital and integral part of every business. It is the gateway to achieve a growing and successful organization. An ideal world class IT department comprises of the following characteristics:

3.1 Security

In the IT world, a secure environment refers to any system which implements the controlled storage and use of information. A "secured" IT environment encompasses several aspects, like'Information Security, 'Information Technology Security', 'Endpoint security' and 'Security Management'.

Based on our observations of <COMPANY HIDDEN>'s existing setup, OEC proposes the following to achieve a secured IT environment:

- XXXX
- XXXX
- XXXX
- XXXX

3.2 Robust Infrastructure

In order to build and grow, an organization must leverage its IT infrastructure to its fullest. To do so, a robust, stable and impregnable IT setup is a critical necessity. A "robust" IT infrastructure incorporates not only steady networking, servers, storage and client machines but also backup/restore, disaster recovery and business continuity plans and solutions.Our audit at <COMPANY HIDDEN> revealed some shortcomings in this area. Below is our proposal for the same:

- XXXX
- XXXX
- XXXX
- XXXX

3.3 Enhance Connectivity:

In today's world, work is not limited within the boundaries of one's physical office. There are several instances when users need to connect to their corporate network from beyond their workplace. This could be for users who are travelling, at a branch office, telecommuters or simply working from home. Based on our findings in <COMPANY HIDDEN>, we recommend the following to enhance connectivity:

- XXXX

- XXXX

3.4 Collaboration

Research has shown that in any organization, employees spend up to 10% of their time every week, looking for information, scheduling meetings and needlessly duplicating communications. This can be reduced tremendously, by use of a collaboration solution that enables users to connect seamlessly across devices and platforms. It should also provide team members the freedom to communicate, collaborate and work efficiently. Our audit revealed the absence of any such solution in the <COMPANY HIDDEN>. Additionally we also observed the lack of a single document storage location.
Our recommendation is as follows:

- XXXX
- XXXX
- XXXX
- XXXX

3.5 Decision Making

The heart of any management process is decision-making. The role of information in decision making cannot be overemphasized. The success of a decision is highly dependent on the information available at the time the decision is made. Management Information System (MIS) provides management with accurate and timely information. This information is required to facilitate the decision-making process and enable organizations to plan, control and operate effectively. MIS may be viewed as a mean for transformation of data to information that can be effectively used in the decision making process. Based on our audit in <COMPANY HIDDEN>, OEC has the following recommendations:

- XXXX
- XXXX
- XXXX

3.6 Standardization

Policies and Standardized Procedures are an integral part of any growing organization. Broadly speaking, “policies” are defined as a predetermined course of action, which is established to provide a guide towards accepted business strategies and objectives. They identify the key activities and provide a general strategy to decision makers on how to handle issues as they arise. A ‘Procedure’ provides the reader with a clear and easily understood plan of action required to carry out or implement a policy.Good procedures allow managers to control events in advance and prevent the organization (and employees) from making costly mistakes.

Our primary observation for <COMPANY HIDDEN> is the XXXX

4 DETAILED FINDING AND RECOMMENDATIONS

Based on the overall work undertaken at the time of the audit, our conclusion on the IT Department is "**Needs Improvement**"

'Needs Improvement' indicates that we believe that a combination of weaknesses in the system of control and non-compliance with the controls in place is such as to place service objectives at risk.

As a result of our audit, **ELEVEN AREAS OF IMPROVEMENT** have been identified which are detailed in this section of the report, together with the recommendations to address these points. The following table summarizes the observations priority wise.

#	Observation	Priority
1	XXXX	
2	XXXX	
3	XXXX	
4	XXXX	
5	XXXX	
6	XXXX	
7	XXXX	
8	XXXX	
9	XXXX	
10	XXXX	
11	XXXX	

1	HIGH	**XXXX**

Finding and implication	**Recommended Action Plan**	**Management Action Plan**
Observations: • XXXX • XXXX • XXXX **Implication& Risks:** • XXXX • XXXX	1. XXXX 2. XXXX 3. XXXX	**Management Response** **Management Action Plan & Due date**

Definition of Impact Ratings

Impact Rating	
HIGH	The opportunity identified is classified as "Must Improve." An observation with High Impact rating needs immediate attention of Management to initiate remedial actions. These opportunities must be implemented.
MEDIUM	The opportunity identified is classified as "Good to Improve." An Observation with Medium Impact rating requires immediate efforts from the Company/Department while taking into considerations financial impact for the organization.
LOW	The opportunity identified is classified as "Recommended." An observation with Low Impact rating is an observation for the Management to consider and an opportunity for continuous improvement.

APPENDIX

#	DESCRIPTION
1.	XXXX
2.	XXXX
3.	XXXX
4.	XXXX
5.	XXXX
6.	XXXX
7.	XXXX
8.	XXXX
9.	XXXX
10.	XXXX
11.	XXXX
12.	XXXX
13.	XXXX
14.	XXXX
15.	XXXX
16.	XXXX