

# **AUDIT REPORT ON**

## **I.S. AUDIT OF CBAS - 2023**

### **Audit Conducted by**

Asfand Yar Javaid (Team Lead)

Ali Asif (Team Member)

## **AUDIT OBSERVATIONS/H2>**

**THE IT-SECURITY POLICY PLACED ON ENB IS FOUND OUTDATED. IT-**

**SECURITY POLICY STATES THAT:**

**“IT SECURITY DEPARTMENT WITH OTHER DEPARTMENTS OF**

**INFORMATION SYSTEMS DIVISION (ISD) SHOULD REVIEW AND**

**UPDATE THE POLICIES AT LEAST ANNUALLY”.**

**HOWEVER, IT IS OBSERVED THAT IT SECURITY POLICY WAS**

**DEVELOPED IN 2013 WHICH HAS NEVER BEEN REVIEWED /UPDATED**

**SINCE THEN.**

**IT IS OBSERVED THAT FOLLOWING DEFINED  
FUNCTIONS ARE NOT BEING PERFORMED AS  
THE RELEVANT EVIDENCES REGARDING  
FOLLOWING DEFINED FUNCTION ARE NOT  
SHARED WITH THE AUDIT:**

**“DESIGNING & DEFINING LOG MANAGEMENT  
PROCEDURES FOR APPLICATIONS, SERVERS,  
AND NETWORK DEVICES IN CASE OF ANY  
INCIDENT HAPPENING IN COLLABORATION  
WITH IT OPERATIONS, IT SYSTEMS  
DEVELOPMENT AND IT NETWORKS.”**

**IT IS OBSERVED THE FOLLOWING DEFINED  
FUNCTIONS ARE NOT BEING PERFORMED AS  
NO RELEVANT EVIDENCES ARE SHARED  
WITH THE AUDIT:**

- **“COORDINATE WITH INTERNAL/EXTERNAL AUDITORS AND ARRANGE COMPLIANCE OF AUDIT OBSERVATIONS PERTAINING TO ISD”**
- **“DESIGNING AND DEFINING ENTERPRISE GROUP POLICIES I.E. ISA SERVERS, AV, FIREWALLS, ETC.”**

**UPON ASSESSMENT OF CYBER SECURITY ACTION PLAN IT IS OBSERVED THAT THE AUDITEE DEPARTMENT REMAIN FAILED IN ACHIEVING FOLLOWING MILESTONES; AS PER SHARED CYBER SECURITY ACTION PLAN (2022), THE IMPLEMENTATION OF PROJECT WAS PLANNED BY Q3-2022.**

1.	<b>ESTABLISHMENT OF CYBER SECURITY OPERATIONS CENTER</b> <ul style="list-style-type: none"> <li>• <b>TO COMPLY THE</b></li> </ul>	<b>3<sup>RD</sup> QUARTER 2022</b>
----	---	--

	<p><b>REGULATORY</b></p> <p><b>REQUIREMENT FOR 24*7</b></p> <p><b>SECURITY MONITORING</b></p> <p><b>THE ESTABLISHMENT OF</b></p> <p><b>SECURITY OPERATION</b></p> <p><b>CENTER WILL BE</b></p> <p><b>ESCALATED WITH</b></p> <p><b>COLLABORATION OF ISD.</b></p>	
2.	<p><b>INFORMATION SECURITY</b></p> <p><b>AWARENESS</b></p> <p><b>• FOR INFORMATION</b></p> <p><b>SECURITY AWARENESS</b></p> <p><b>ACROSS THE BOARD TO ALL</b></p> <p><b>ZTBL EMPLOYEES,</b></p> <p><b>LEARNING MANAGEMENT</b></p> <p><b>SYSTEM SHALL BE</b></p> <p><b>ACQUIRED/IMPLEMENTED</b></p>	<p><b>3<sup>RD</sup></b></p> <p><b>QUARTER</b></p> <p><b>2022</b></p>

<b>WITH INFOGRAPHICS</b>	<b>CONTENTS.</b>
--------------------------	------------------

**IT IS OBSERVED THAT THAT 2 X DIFFERENT POLICES ARE  
AVAILABLE ON ENB I.E. REVISED IT- SECURITY POLICY (2013) AND  
INFORMATION/CYBER SECURITY POLICY.**

**AS PER SHARED EVIDENCE REGARDING 3<sup>RD</sup> PARTY VULNERABILITY  
ASSESSMENT AND PENETRATION TESTING (VAPT) IT IS OBSERVED  
THAT THE 3<sup>RD</sup> PARTY VAPT EXERCISE WAS CONDUCTED ON 28-  
FEBRUARY-2022 AND NUMBER OF HIGH RISK VULNERABILITIES  
WERE ADDRESSED IN VAPT REPORT.**

**HOWEVER, NO VAPT REASSESSMENT CERTIFICATE TO ENSURE THE  
MITIGATION OF HIGHLIGHTED RISKS/VULNERABILITIES IS SHARED  
WITH THE AUDIT TEAM.**

**CLAUSE 5.3.1 “DISASTER RECOVERY PLAN” OF SBP CIRCULAR C-5  
STATES:**

**“EVALUATE THE RECOVERY PLAN AND INCIDENT RESPONSE  
PROCEDURES AT LEAST ANNUALLY AND UPDATE THEM AS AND  
WHEN CHANGES TO BUSINESS OPERATIONS, SYSTEMS AND  
NETWORKS OCCUR.**

**HOWEVER, UPON ASSESSMENT OF DR&BCP  
DRILL REPORT 2021, IT IS OBSERVED THAT  
THE AVAILABILITY OF ATM/ADC SERVICES  
FROM DR SITE IS NOT TESTED DURING  
EXERCISE AS THE SHARED DR&BCP REPORT  
DOES NOT SHOW THE TESTING OF ATM/ADC  
SERVICES FROM DR SITE.**

**IT IS OBSERVED THAT DEPARTMENTAL  
FUNCTIONS SHARED BY AUDITEE  
DEPARTMENT ARE DIFFERENT FROM  
APPROVED HR-FUNCTIONS AS THE  
FOLLOWING APPROVED FUNCTIONS ARE**

**MISSING IN SHARED DEPARTMENTAL MAIN  
FUNCTIONS:**

- **PLAN AND COORDINATE ALL ACTIVITIES  
RELATED TO BCP/DRP DRILL(S).**
- **CONDUCT PERIODIC REVIEWS OF USERS'  
ACCESS/SPECIAL PRIVILEGES, SYSTEMS  
AUDIT TRAIL LOGS AND CONFIGURATION  
CHANGES WITHIN INFORMATION SYSTEMS.**
- **DEFINE LOG MANAGEMENT PROCEDURES  
FOR APPLICATIONS, SERVERS, AND  
NETWORK DEVICES.**

**AT ZTBL NETWORK ENVIRONMENT, A CENTRALIZED DEDICATED  
PROXY SERVER IS CONFIGURED TO SHARE SECURE INTERNET  
SERVICES THROUGHOUT THE ORGANIZATION AND THE BANK IS  
PAYING MONTHLY RECURRING CHARGES TO INTERNET SERVICE  
PROVIDER (ISP) FOR THIS INTERNET SERVICE AND FOR MANAGED  
NETWORK AT BRANCH OFFICES.**

**HOWEVER, IT IS OBSERVED THAT AT ZTBL BRANCH OFFICES,  
INSTEAD OF USING ONLY THIS OFFICIAL INTERNET CONNECTION,  
USE OF 3<sup>RD</sup> PARTY SERVICE LIKE DSL IS ALSO IN PRACTICE WHICH  
VIOLATES THE IT SECURITY POLICY:**

**“EMPLOYEES ACCESSING THE INTERNET  
USING COMPUTERS OF THE BANK ARE NOT  
PERMITTED TO ATTACH TO THE INTERNET  
THROUGH SOURCES OTHER THAN THE  
BANK’S INTERNET COMMUNICATION  
FACILITIES WITHOUT PRIOR REVIEW AND  
APPROVAL FROM THE IT SECURITY  
DEPARTMENT. HOWEVER, IN CASE OF  
EMERGENT SITUATION, LIMITED TIME  
APPROVAL WOULD BE GRANTED”.**

**PROVISION OF INTERNET SERVICE THROUGH  
DSL DEVICES PUTS THE BANK’S OVERALL**



**NETWORK SECURITY AT RISK AS NO  
CENTRAL CONTROLS CAN BE IMPLEMENTED.  
MOREOVER, THE BANK HAVE TO SUFFER  
THE BURDEN ADDITIONAL COST FOR SUCH  
SERVICES.**

**CYBERSECURITY HYGIENE EXERCISE WAS CONDUCTED DURING THE  
MONTH OF MAY-2022 AS PER DIRECTIONS OF SBP. HOWEVER, IT IS  
OBSERVED THAT THE STATUS OF SBP “CYBER HYGIENE SELF-  
ASSESSMENT EXERCISE” IS NOT SHARED WITH AUDIT TEAM.**