INFORMATION SYSTEM AUDIT REPORT ON INTEGRATED EDUCATION MANAGEMENT INFORMATION SYSTEM (iEMIS) ELEMENTARY & SECONDARY EDUCATION DEPARTMENT GOVERNMENT OF KHYBER PAKHTUNKHWA

AUDIT YEAR 2023-2024

AUDITOR-GENERAL OF PAKISTAN

SERVING THE NATION BY PROMOTING ACCOUNTABILITY, TRANSPARENCY AND GOOD GOVERNANCE IN THE MANAGEMENT AND USE OF PUBLIC RESOURCES FOR THE CITIZENS OF PAKISTAN

PREFACE

The Auditor-General of Pakistan conducts audit in terms of Articles 169 and 170 of the Constitution of the Islamic Republic of Pakistan 1973, read with sections 8 and 12 of the Auditor-General's (Functions, Powers and Terms and Conditions of Service) Ordinance 2001. The IS audit of Integrated Education Management Information System (iEMIS) of Elementary & Secondary Education Department (E&SED), Khyber Pakhtunkhwa Peshawar, was carried out accordingly.

The Directorate-General Audit (Local Governments) Khyber Pakhtunkhwa Peshawar conducted the IS audit of iEMIS, E&SED, Khyber Pakhtunkhwa during Audit Year 2023-24 with a view to report significant findings to stakeholders. Audit assessed the adequacy, effectiveness, and efficiency of internal controls in place to determine whether the systems and applications are aligned with the entity's needs, operate efficiently, and are sufficiently controlled to mitigate risks and ensure reliable operations. In addition, audit also assessed, on test check basis whether the management complied with applicable laws, rules and regulations in developing and managing the project affairs. The Audit Report indicates specific actions that, if taken, will help the management realize the objectives of the organization. All observations included in this report have been finalized in the light of discussion with the management.

PAO (Secretary Education KP) was requested to convene DAC meeting in July 2024, which could not be convened till finalization of this report.

The IS Audit Report is submitted to the Governor of Khyber Pakhtunkhwa in pursuance of Article 171 of the Constitution of the Islamic Republic of Pakistan 1973, for causing it to be laid before the Provincial Assembly.

(Muhammad Ajmal Gondal)
Dated: **Auditor-General of Pakistan**

TABLE OF CONTENTS

ABBREVIATIONS & ACRONYMS

APO	Align, Plan and Organize
ASC	Annual Schools Census
ASDEO	Assistant District Education Officer
BAI	Build, Acquired and Implement
BCP	Business Continuity Plan
COBIT	Control Objectives for Information and related Technologies
DAC	Departmental Accounts Committee
DE&SE	Director Elementary & Secondary Education
DEO	District Education Officer
DRP	Disaster Recovery Plan
E&SED	Elementary & Secondary Education Department
EMA	Education Monitoring Authority
EMIS	Education Management Information System
ESDSS	Education Spatial Decision Support System
ESPIG	Education Sector Program Implementation Grant
FAC	Further Audit Comments
GPE	Global Partnership for Education
IAM	Identity and Access Management
iEMIS	Integrated Education Management Information System
IMU	Independent Monitoring Unit
ISO	International Organization for Standardization
KPEIP	Khyber Pakhtunkhwa Education Improvement Program
KPEMA	Khyber Pakhtunkhwa Education Management Authority
MFA	Multi-Factor Authentication
MUST	Management Unit for Study and Training
P&P	Policies and Procedures
RPO	Recovery Point Objectives
RTO	Recovery Time Objective

SDA	System Development and Acquisition
SDLC	Software Development Life Cycle
SE&SE	Secretary Elementary & Secondary Education
SFA	Single-Factor Authentication
SOPs	Standard Operating Procedures
SRS	Software Requirement Specification
SSL	Secure Socket Layer
USAID	United State Agency for International Development

EXECUTIVE SUMMARY

Overview

An audit team constituted by the office of the Auditor-General of Pakistan consisted of one director, two audit officers taken from Directorates-General Audit (Local Governments & Social Safety Nets) and one foreign consultant. The team conducted Information System Audit of integrated Education Management Information System (iEMIS) of Elementary & Secondary Education Department (E&SED), Khyber Pakhtunkhwa (KP). The main objectives of the audit were to i) check the IT Governance for effective management of software ensuring alignment with educational objectives, efficient resource management, ii) evaluate the process of Information Systems development, acquisition and implementation for ensuring the formal software development lifecycle, quality assurance, and controlling configuration changes, iii) check the adherence of information system outsourcing and operations with applicable laws, regulations, and international established best practices, iv) examine the information security system, its robustness, reliability of the IS infrastructure and network infrastructure to ensure the integrity and security of the systems and applications. The audit was conducted in accordance with the International Standards of Supreme Audit Institutions Guidelines on IS Audit (ISSAI 5100).

The Education Management Information System (EMIS) Cell of E&SED, KP developed iEMIS based on the Software Requirement Specification (SRS) for key systems within E&SED under Khyber Pakhtunkhwa Education Improvement Program (KPEIP) funded through Education Sector Program Implementation Grant (ESPIG) of Global Partnership for Education (GPE). The SRS document was approved by E&SED as a living document in January 2023. As part of roadmap of SRS document and phase wise implementation plan of the iEMIS, it was imperative to initiate implementation of prioritized systems within E&SED. For this purpose, EMIS cell developed operational plan proposing to strategize

and align E&SED's structure from Provincial to District Education Officer (DEO) levels for effective rollout, implementation and use of iEMIS.

By integrating various data systems with EMIS, the Provincial EMIS Cell aims to create a unified platform that would effectively handle different aspects of the educational information. This integration would likely lead to better data sharing, analysis, and decision-making processes.

The integration and development activities were performed in-house so as to allow greater control over the development process, customization according to specific needs, and the ability to address any issues promptly.

Conclusion

The Information Systems (IS) audit results revealed that essential IT strategies, policies, and procedures were lacking. The audit scope testing areas, including IT Governance, System Development & Acquisition, IT Operations, Information Security, and Business Continuity & Disaster Recovery Plan, exposed significant shortcomings. These deficiencies make the system less efficient, less effective, and less economical in the following ways:

System Efficiency (Automated vs Manual)	IT* Governance	Service Delivery
Mostly Manual	**Poor**	**Dissatisfied**

(Rating matrix that was used for classification is attached as Appendix IS-R to the report)

The integrated Education Management Information System (iEMIS) suffers inefficiencies due to poor data management and analysis, resulting in inaccurate or incomplete data, which may lead to poor decision-making. It is crucial to address the issue of student enrollments plan and timelines in the province effectively. Additionally, the reliance on outdated hardware and a single machine (server) has greatly diminished the system's performance.

The EMIS proves ineffective in remote regions of the province due to limited internet connectivity and poor signal strength, which restricts access to the

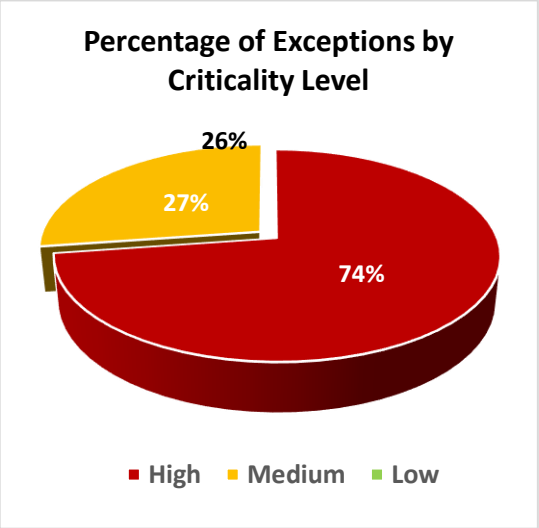
system. This renders the system ineffective for schools and educational administrators in these areas, as they are unable to access crucial data and information needed for their decision-making. As a result, educational planning, monitoring, and evaluation face challenges, which can affect the overall quality of education in these areas. The unavailability of the EMIS in these areas undermines its purpose and highlights the need for innovative approach to ensure inclusive and equitable access to educational information and resources.

Additionally, the lack of a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) can have adverse consequences for the Education Management Information System (EMIS), leading to significant financial losses, reputational damages, and other severe impacts in education department. In the event of a disaster or system failure, the lack of a BCP and DRP would mean that critical educational data could be lost forever, causing harm to efficacy of evidence-based decision-making in the education sector. Moreover, the financial costs of rebuilding and recovering the system could be exorbitant, diverting resources away from essential educational initiatives. Furthermore, the loss of personal data of students, teachers, and parents, could lead to legal and reputational repercussions. The absence of a BCP and DRP could also disrupt educational operations in case of a crisis situation or a disaster, causing delays and cancellations of critical activities, and undermining the effective functioning of educational initiatives in the province.

OVERALL RESULTS

To enable management towards setting priorities on their action plans, the audit observations are reported in three categories i.e. High, Medium and Low risks. Exceptions rating matrix that was used for classification of observations is attached as Appendix IS-R to the report.

Audit Rating	Number of Observations
High	17
Medium	6
Low	0
Total	23



A summary of the audit observations raised during the course of the review is reflected in the tabulated form as given below:

SUMMARY OF OBSERVATIONS

Ref	Observation	High	Medium	Low
4.1	**IT Governance**			
4.1.1	Absence of IT Strategic Plan	□		
4.1.2	Lack of IT Policy and Procedures	□		
4.1.3	Absence of IT Steering Committee	□		
4.1.4	Non-Availability of IT Organizational Structure / Chart	□		
4.1.5	Insufficient Segregation of Duties within the IT Department	□		
4.1.6	Insufficient IT Risk Management Processes	□		
4.2	**Information Systems Development and Acquisition**			
4.2.1	Lack of Formal Software Development Life Cycle (SDLC) Methodology		□	

4.3	**Information Systems Operations, Maintenance, and Support**			
4.3.1	Weak IS Operations, Maintenance, & Support	□		
4.3.2	Absence of Formal Change Management Process in System	□		
4.3.3	Multiple Critical Services of iEMIS on Single Server	□		
4.3.4	Absence of Formal IT Assets Management Process		□	
4.4	**Information Security**			
4.4.1	Absence of Formal User Access Management	□		
4.4.2	Excessive SUPER ADMIN Accounts and Misuse of Privileges	□		
4.4.3	Lack of Regular User Account Review and Recertification		□	
4.4.4	Weak Password and Session Controls	□		
4.4.5	Lack of Standard System Baseline Configuration	□		
4.4.6	Absence of Encryption for Sensitive Data Transmission	□		
4.4.7	Oracle Database Port Publicly Accessible	□		
4.4.8	Insufficient Authentication Mechanism	□		
4.4.9	Absence of Performing Regular Penetration Testing		□	
4.4.10	Weak Physical and Environmental Controls in Datacenter		□	
4.5	**Business Continuity and Disaster Recovery**			
4.5.1	Absence of Business Continuity and Disaster Recovery Plan	□		
4.5.2	Absence of Formal Process for Managing Tapes and Removable Media		□	
Total		**17**	**6**	**0**

1. INTRODUCTION

1.1 Background

EMIS in KP was initiated under the USAID-funded Management Unit for Study and Training (MUST) Project in the late 1980s. It was properly established in 1990-91 in the Directorate of Primary Education to cover Primary Level Schools only and expanded to cover Secondary Schools in 2002 after the merger of Primary & Secondary Education under the control of Director Elementary & Secondary Education (DE&SE). It was restructured in 2006 under the direct control of Secretary Elementary & Secondary Education (SE&SE), but later, in 2014, it went under Khyber Pakhtunkhwa Education Management Authority (KPEMA). Education Management Information System (EMIS) evolved over the years, expanding to cover secondary schools and undergoing restructuring. The EMIS cell developed annual statistical reports and conducted the Annual Schools Census (ASC). However, the existing system had limitations, including a distributed MS Access environment, desktop-based offline system, and manual data merging.

To address these limitations, an online Education Spatial Decision Support System (ESDSS) was developed with features of online data entry, real-time reports, automated data merging, and quality control. However, the ASC responsibility was shifted to the Independent Monitoring Unit (IMU), now the Education Monitoring Authority (EMA), in 2016-17.

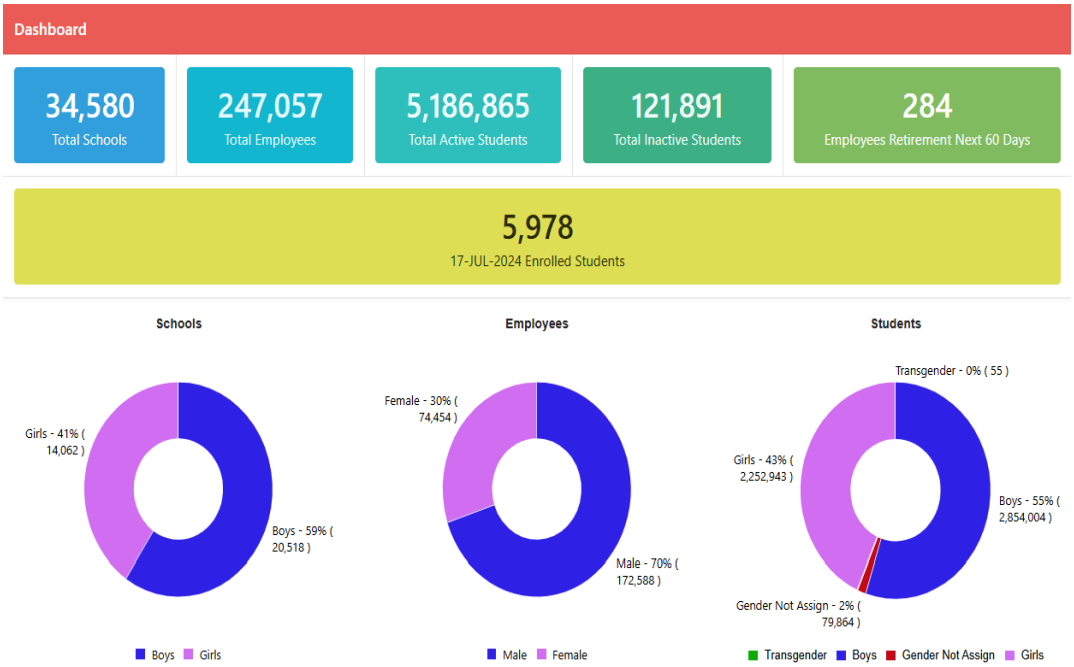
The EMIS cell of ESED developed an integrated Education Management Information System (iEMIS), to digitally connect all its attached institutions in order to facilitate informed decision-making, better planning, monitoring, evaluation and student learning outcomes.

1.2 Summary of Integrated Education Management Information System

The Elementary & Secondary Education Department (E&SED) oversees more than thirty-four thousand public sector education institutions at primary and secondary level across Khyber Pakhtunkhwa. These institutions impart education to five million students with the assistance of two hundred and forty-seven thousand employees (see iEMIS dashboard below).

As part of system strengthening, the Department focused on creating stronger data streams that come together in an information management system.

To achieve this, the Provincial EMIS Department developed a system called iEMIS which stands for "Integrated Education Management Information System". The iEMIS is a tool for Data collection, Storage, Integration, Analysis and Dissemination; specifically designed for use by planners and administrators to plan and administer education system more efficiently and effectively.



The integrated Education Management Information System (iEMIS) was developed by the Department to digitally connect all its attached institutions in order to facilitate informed decision-making, better planning, monitoring, evaluation and student learning outcomes.

The EMIS Cell of E&SED KP proposed a phased implementation plan, starting with operationalizing three core modules:

- Office/School MIS,
- HR MIS, and
- Student MIS.

The scope and objectives of iEMIS is as follows:

- **Scope**: The scope of the integrated Education Management Information System (iEMIS) is to strengthen the efficiency and governance at all levels within E&SED using data and consistent flow of information for informed planning, management and decision-making.
- **Objectives:** The primary objective is to automate, digitize and integrate the process of data collection, management and dissemination. Other objectives include data integration, data validation, reporting, data visualization, planning and monitoring and user management.

The current IT/EMIS setup in E&SED includes a Provincial EMIS (PEMIS) team responsible for developing and coordinating IT/Data Systems. However, there is a need to strengthen IT-related operations, improve efficiency, and maximize staff expertise.

1.3 Financial Data

The financial data regarding hiring and procurement was asked for from the management through letter No. F-202/M&E/Misc/2023-24/01 dated 26.06.2024, first reminder dated 09.07.2024 and 2nd reminder dated 23.07.2024 of even numbers. The management through it's letter EMIS/E&E//1-4/General dated 24.07.2024 replied as follows:

"Education Management Information System is an integral part of Elementary & Secondary Education (E&SE) Department like other sections of E&SE Department and has no separate administrative setup and no separate budget for procurement and hiring of staff. The EMIS section receives IT's equipment's E&SE Department departmental period purchasing like other sections of the E&SE Department. Moreover, Establishment and Administration Department, Government of Khyber Pakhtunkhwa hires/posts technical staff for all Departments, including E&SE Department as well."

"The management's response was not tenable as it failed to provide any financial information regarding hiring and procurement activities, despite repeated requests from the audit team. The audit team maintains that all expenditures incurred by the E&SE Department, regardless of the means of procurement, constitute public

funds and are therefore subject to audit scrutiny. It was incumbent upon the department to ensure the availability of requisite information and facilitate a comprehensive audit examination."

2. AUDIT OBJECTIVE

The primary objectives of the Information System audit were:

- To check the IT Governance for effective management of software ensuring alignment with educational objectives, efficient resource management
- To evaluate the process of Information Systems development, acquisition and Implementation for ensuring the formal software development lifecycle, quality assurance, and controlling configuration changes
- To check the adherence of information system outsourcing and operations with applicable laws, regulations, and international established best practices
- To examine the information security system, its robustness, reliability of the IS infrastructure,
- To examine maintenance & support system
- To check the business continuity plan and disaster recovery plan.

3. AUDIT SCOPE AND METHODOLOGY

The review was conducted with focus on achieving goals related to understanding and evaluating the effectiveness and efficiency of the IT General Controls applicable for in-scope application – Integrated Education Management Information System (iEMIS), in respect of the following:

- **Information Technology Governance**: IT governance principles to ensure alignment of IT and business goals, optimized use of IT resources, improved risk management, enhanced decision-making, and regulatory compliance.
- **Information Security:** Information security related controls like password parameters, audit trails, user access management, and administrator level logical access controls.
- **Information Systems Operational Resilience**: Backups, offsite data storage, monitoring of scheduled jobs, performance monitoring, help desk support, physical and environmental controls in the data center / server room.
- **Change Management Control**: Change management life cycle for in scope applications from initiation of a change request to approval, development, testing, and implementation of the change in production instance.
- **Application Control (Input, Process, and Output)**: Verify accuracy, completeness, validity, and security of data as input, processed, and output in order to maintain data integrity and ensure that the application is functioning as intended.

This audit review was conducted in conformance with the Auditor General of Pakistan Information Systems Audit Methodology and International Standards for the Professional Practice of Information Systems Auditing. Refer to Appendix IS-1 for Terms of Reference (ToR) document.

4. AUDIT FINDINGS & RECOMMENDATIONS

4.1 IT GOVERNANCE

IT Governance is essential for education department for effectively managing software, ensuring risk mitigation, efficient resource management, performance management and alignment with educational objectives for valuable delivery of services. It promotes accountability, transparency, and compliance with regulations, while also driving continuous improvement and scalability. With IT Governance, the department can make informed decisions, optimize resource allocation, and ensure software quality and reliability. This leads to improved stakeholder engagement, better decision-making, and ultimately, supports the delivery of high-quality education and research. By implementing IT Governance, the education department can harness the full potential of software to enhance teaching, learning, and administrative processes, while minimizing potential risks and errors. However, while conducting IS audit of iEMIS of Elementary & Secondary Education Department KP, audit observed there was no governing body formed which could be responsible for making strategic decisions for IT. IT Governance framework is given below:

IT Governance Framework

Consequently, audit observed a lot of shortcomings as detailed below:

Category: Information System (IS)/Information Technology (IT) related issues

4.1.1 Absence of IT Strategic Plan	High

Pakistan's National IT Policy 2000, (Section 3.4.1.4.3) stipulates that "a comprehensive plan for education and human resource development in IT shall be drawn up to meet the present and future needs of manpower".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the IT department is currently operating without a formal IT strategic plan. There was no documented strategy to guide IT investments, prioritize projects, or align IT initiatives with educational goals. Additionally, IT projects are often initiated on an ad-hoc basis without a cohesive vision, leading to fragmented systems and inconsistent performance.

The absence of an IT Strategic Plan leads to inefficient use of resources, inadequate support for business operations, and increased risk of errors, which result in inefficacy, reputational damage, and financial losses. Moreover, it also hinders the organization's ability to keep pace with changing technology and business needs, compromising data security and integrity.

When pointed out by Audit in July 2024, the management replied that "the Government of Khyber Pakhtunkhwa is currently developing an IT strategy to implement e-Governance across the province. This initiative aims to integrate the processes of all departments to enhance efficiency and service delivery. As part of the provincial government, the Elementary & Secondary Education Department will definitely implement the same within its comprehensive framework."

The management's reply was not convincing as the department failed to develop a comprehensive IT Strategic plan within the education department. No progress was shown to audit till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends developing comprehensive IT Strategic Plan aligned with organization strategy.

4.1.2 Lack of IT Policy and Procedures — High

Pakistan's National IT Policy 2000, (Section 3.4.1.4.3) stipulates that "a comprehensive plan for education and human resource development in IT shall be drawn up to meet the present and future needs of manpower".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that there were no formally defined IT policies and procedures (P&P), with either no documentation or unapproved documentation by the management. Consequently, essential policies and procedures, including the following but not limited to, were missing or inadequate, and were not supported by checklists to show evidence of work performed and reviews conducted:

Policy	Procedure
• Acceptable User Policy (AUP) • Access Control • Data Protection • Information Security • Backup and Recovery • Incident Response • Change Management • Software and Hardware Management • Remote Access • Network Security • Disaster Recovery • IT Asset Management	• User Access Management • Data Back • Incident Handling • Audit Logging • Patch Management • Password Management • System Monitoring • Change Request • Service Desk • Network Configuration • Data Retention and Disposal • IT Training and Awareness

The lack of documented policies and corresponding procedures approved by IT management may lead to inconsistent implementation of IT operations and activities across the organization.

When pointed out by Audit in July 2024, the management replied that "presently the ST&IT department is working on Provincial IT Digital Policy wherein rules and procedures of all line departments will be clearly documented and E&SE department will accordingly follow those procedures as per approved provincial IT Digital Policy."

The management's reply was not satisfactory as there were no formally defined IT policies and procedures in Elementary & Secondary Education Department. No documents were provided in support of reply till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends that E&SED KP should establish comprehensive and formally documented internal IT policies and procedures manual that covers all areas related to IT.

4.1.3 Absence of IT Steering Committee	**High**

Control Objectives for Information and related (COBIT)-5 (Roles and Organizational Structures), defines the steering committee as a group of stakeholders and experts who are accountable for guidance of programme and projects, including management and monitoring of plans, allocation of resources, delivery of benefits and value, and management of programme and project risk.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the Education Department did not have a steering committee or any other management committee established to oversee and govern its IT initiatives.

Non-establishment of IT Steering Committee resulted in unawareness of the management for making the business decision regarding selection of technology and may lead to poor alignment of IT strategy with business objectives, limited IT transparency and accountability.

When pointed out by Audit in July 2024, the management stated that "the observations are well noted and the draft composition and TORs of IT Steering

committee at the E&SE department level would be developed in line with the approved KP IT Digital Policy for proper approval and notification."

The management acknowledged the observations and made a commitment to develop composition and draft TORs for the IT Steering Committee. However, no progress was shown to audit till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends E&SE Department KP to establish a steering committee to oversee IT initiatives.

4.1.4 Non-Availability of IT Organizational Structure / Chart	**High**

The COBIT-5 (Governance and Management) framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not have a defined IT organizational structure/chart, which is a critical component of effective IT governance.

The absence of a defined IT organizational structure/chart resulted into ineffective IT governance, inadequate resource utilization, and limited accountability, resulting in increased risk and decreased efficiency.

When pointed out by Audit in July 2024, the management stated that "IT organizational structure is already in place and there is a Provincial IT Cadre in the Establishment Department for all IT HR in the line departments. Copy of the Establishment Department IT Structure is at Annex-I, hence the same organizational structure is also for IT staff in the E&SE Department."

The management's reply was not convincing as the department was relying on the Provincial IT Cadre rather than having its own IT Organizational structure/ setup. Alternatively, the management could not provide evidence of how and to what extent it had control over functioning of IT resources acquired from provincial IT Cadre including assignment of responsibilities and accountability.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the management to develop a comprehensive IT organizational structure/chart with clearly defined roles and responsibilities and align IT resource allocation with organizational objectives.

4.1.5 Insufficient Segregation of Duties within the IT Department	**High**

ISO 27001 (Controls), internal organization, (Section A.6.1.2) mandates that "conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization assets".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that there was insufficient segregation of duties within the IT department. For instance, the software developer performs multiple duties, including but not limited to software development, database administration, user access management, and end user support.

The lack of proper segregation of duties exposes the organization to several risks, including increased risk of fraud and error, compromised system integrity, weak accountability, and operational inefficiencies.

When pointed out by Audit in July 2024, the management replied that "IT section is an integral part of E&SE department and is not a separate department. IT section of E&SE department within its limited HR technical resources from its parent department (i.e. Establishment Department) performs multiple assignments as per their expertise and requirements. In line with the

recommendations, the E&SE department has already requested and will again process case for creation/provision of more technical HR resources to the Establishment/ Finance Departments."

The management's reply was not convincing as the management failed to produce any documentary evidence in support of reply.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to mitigate the risks associated with insufficient segregation of duties by reassessing staffing needs, defining roles and responsibilities for all IT team members.

4.1.6 Insufficient IT Risk Management Processes	High

COBIT-5 (Roles and Organizational Structure), defines that the most senior official of the enterprise who is accountable for all aspects of risk management across the enterprise. An IT risk officer function may be established to oversee IT-related risk.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization's IT risk management processes were insufficient, with significant gaps in risk identification, assessment, mitigation, and monitoring as there was no formal IT risk management framework or policy in place. Thus, without IT risk management framework/policy the chances of IT risks like hardware software failure, human error, spam, viruses and malicious attacks could not be ruled out.

The insufficient IT risk management process can damage the reputation, trust among stakeholders and inadequate risk management can lead to unanticipated disruptions in IT operations, affecting the availability and reliability of the iEMIS.

When pointed out by Audit in July 2024, the management stated that "presently all the development in the IT/EMIS section of E&SE department is done in-house

and 2 to 3 technical HRs are already involved for backup development. As far as advance trainings and more HRs are concerned there are limitations of resources / separate budget".

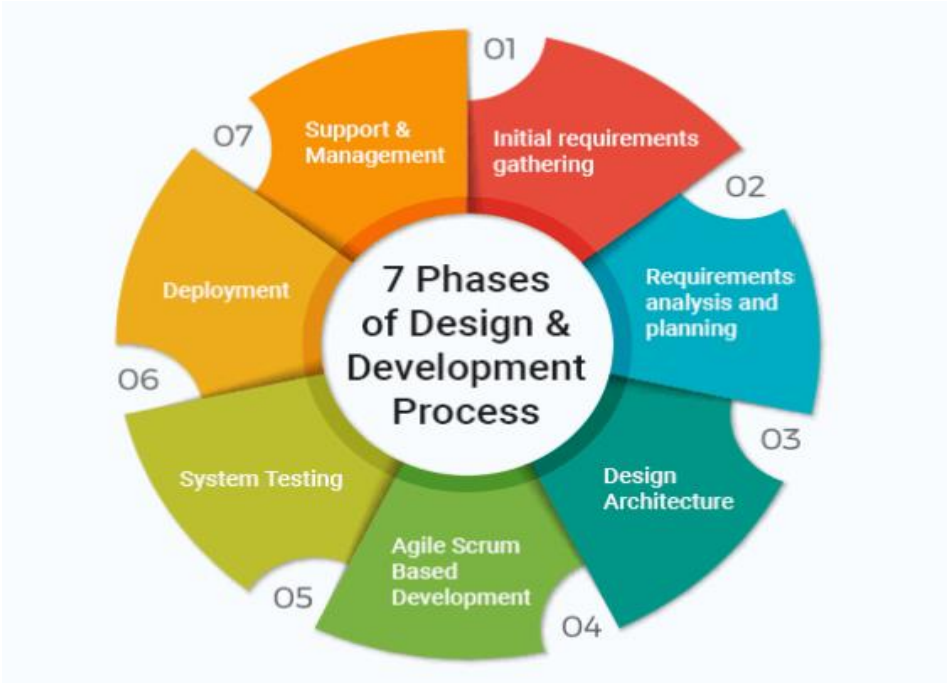
The management's reply was not convincing as without IT risk management framework and advance trainings of HRs, the chances of IT risks like hardware software failure, human error, spam, viruses and malicious attacks could not be ruled out.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to establish a comprehensive IT risk management policy and framework based on recognized standards (e.g., ISO 31000, NIST SP 800-37) – including risk identification, risk assessment, risk mitigation, and risk monitoring.

4.2 INFORMATION SYSTEMS DEVELOPMENT & ACQUISITION

System Development and Acquisition (SDA) is a comprehensive process that encompasses the entire lifecycle of an information system, software application, or technology solution. As shown in the diagram below, it begins with planning, where requirements are defined, and needs are identified, followed by analysis, where functional and technical specifications are outlined. The design phase creates a detailed blueprint of the system, including architecture, components, and interfaces. Development involves building the system, including coding, testing, and integration. Testing verifies that the system meets requirements, and deployment installs, configures, and deploys the system to production. Maintenance updates, modifies, and supports the system over its lifespan. Acquisition, on the other hand, involves procuring a system, software, or technology solution from an external vendor, developer, or supplier, including requirements gathering, vendor selection, contract negotiation, implementation, testing, and acceptance. Effective SDA is critical to developing and acquiring systems that meet business needs, improve operations, and drive innovation. In the following section, audit has highlighted the observations related to system development & Acquisition.



Software Development Life Cycle (SDLC) Diagram

4.2.1 Lack of Formal Software Development Life Cycle (SDLC) Methodology	Medium

ISO 27001, (System Acquisition, Development and Maintenance), (Clause A.14.2) requires “ensuring that information security is designed and implemented within the development lifecycle of information systems”. ISO 27001, (System Acquisition, Development and Maintenance), (Clause A.14.2.2) provides that “changes to system within the development lifecycle shall be controlled by the use of formal change control procedures”.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the entity did not have a formal process for developing, implementing, and maintaining systems, managing projects, ensuring quality assurance, and controlling configuration changes, which resulted in weak Project Initiation Phase, Weak Project Planning, and Weak Project Implementation. This lack of a structured SDLC methodology has resulted in several issues, including inconsistent development practices, inadequate project management, poor quality assurance, and insufficient configuration control.

Without a formal SDLC, the organization was at risk of developing software with poor quality and security vulnerabilities, including unauthorized changes, conflicts, and difficulties in maintaining system integrity. Moreover, lack of structured project management processes could also lead to project delays, cost overruns, and failure to meet project objectives.

When pointed out by Audit in July 2024, the management agreed with the observations and recommendations and stated that up to some extent, the SDLC requirements have been met during the development of the iEMIS.

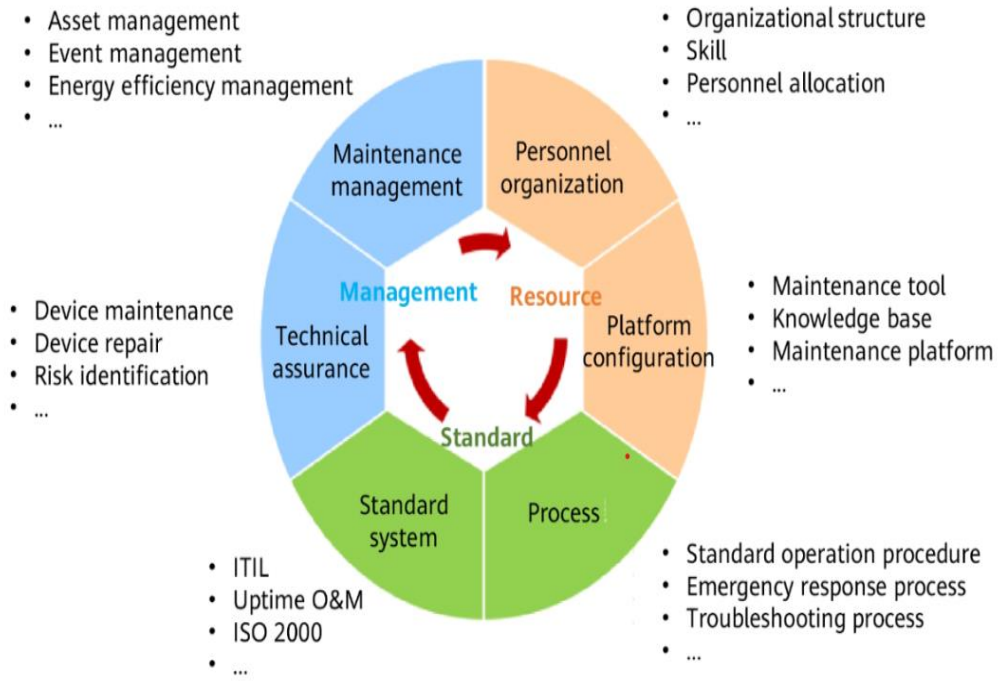
The management's response was inadequate as formal SDLC was essential for a reliable and secure system. No progress was shown in the matter till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to develop and implement formal SDLC framework while defining clear phases such as planning, requirements analysis, design, development, testing, deployment, and maintenance.

4.3 INFORMATION SYSTEMS OPERATIONS, MAINTENANCE, AND SUPPORT

IS Operations refers to the day-to-day management and maintenance of an organization's IS infrastructure, systems, and services. It encompasses a broad range of activities, including monitoring and troubleshooting, incident management, problem management, change management, configuration management, and release management. IS Operations ensures the smooth operation of IS services, minimizing downtime and maximizing performance, security, and efficiency. This includes managing data centers, networks, servers, databases, applications, and end-user services, as well as providing technical support and help desk services to employees and customers. Effective IS Operations is critical to business continuity, ensuring that IS services are delivered consistently, reliably, and securely, and that IT assets are utilized optimally. By streamlining IS Operations, organizations can improve productivity, reduce costs, and enhance the overall user experience.



IS Operations and Maintance

(Source: Genral O&M Management)

4.3.1 Weak IS Operations, Maintenance, & Support	High

Digital Pakistan Policy (Section 10.4) "recommends efficient governance, focused platforms for identity/transaction management, payment mechanism, digital documentation etc".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the entity did not have a formal and documented IS Operations Policy that outlines the guidelines, procedures, and responsibilities such as the IT operations and lacked essential planning, oversight, and monitoring. Key gaps included the absence of an IT operations plan, undefined service metrics and quality standards, and no performance monitoring or reporting. Furthermore, system configurations were not documented, and there was no incident response team or escalation mechanism in place. Additionally, user training on incident response was inadequate, hindering effective IT operations and incident management.

This lack of policy framework leads to inadequate management of IT services, inefficient incident management and problem resolution, uncontrolled changes to IT systems and services, and inadequate configuration management.

When pointed out by Audit in July 2024, the management stated that the objections raised are standard norms for any IT system development and implementation. The EMIS/IT Section within E&SE Department despite its limitations elaborated in the previous replies, have done/complied most of the norms during development and operationalization of the iEMIS. e.g.

1. There is Software Requirements Specifications (SRS) covering both the hardware and software. Copy already shared with Audit team.
2. Standard Operating Procedures (SOP) for implementation and usage of the iEMIS (Annex-III).
3. Roles / Responsibilities defined of all the IT/technical staff within E&SE department from Provincial up to school level (Annex-IV).

The management's reply is not convincing as the department did not have a formal and documented IS Operations & Maintenance Policy. No documentary evidence was provided in support of the reply.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends that the entity develop and implement a comprehensive IS Operations & Maintenance Policy that outlines the guidelines, procedures, and responsibilities for managing IT operations.

4.3.2 Absence of Formal Change Management Process in System	High

Pakistan National Cyber Security Policy 2021, (Clause 3.8) states that "Research & Development programs shall address all aspects including the development of Cyber Security systems, testing, deployment, and maintenance throughout the life cycle".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not have a formal change management process and there was no evidence that changes to the IT infrastructure, applications, and services were made with proper assessment, approval, and implementation controls. Furthermore, all the changes to iEMIS were being made on the production environment rather than on testing environment. Audit further observed that there was no sandbox environment for iEMIS in place.

The absence of a change management policy poses a significant risk to business operations, leading to potential disruptions, errors, and financial losses. Implementing a change management policy is essential to ensure continuity and integrity of business operations.

When pointed out by Audit in July 2024, the management stated that "the recommendations are well noted. Hopefully these will be addressed with the development of a comprehensive IT strategy and policy.

The management's reply was not convincing as the department did not have a formal Change Management Process in System. No documentary evidences regarding the existence of a formal Change Management Process in System were furnished till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the management to develop and implement a comprehensive change management policy that includes procedures for assessing, planning, executing, and documenting changes.

4.3.3 Multiple Critical Services of iEMIS on Single Server	**High**

Pakistan National Cyber Security Policy 2021, (Clause 3.5), encourages the establishment of national Data Centers to co-locate servers and telecom Quality infrastructure for all government entities - federal & provincial. Furthermore, it mandates to define and enforce a robust Government Authentication and Data Protection Framework including data classification and to ensure that appropriate controls exist to protect data.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization's database server, application server, and web server were all running on a single physical server instead of separate servers for each service. This practice introduces several risks and challenges related to performance, security like unauthorized access and disaster recovery.

This poses a significant risk to security, performance, and availability. A single vulnerability in any component could compromise the entire system. Furthermore, a denial-of-service attack on the web server could impact database and application performance and a security breach in one component could spread to others.

When pointed out by Audit in July 2024, the management stated that currently for the iEMIS, a shared Server at the KP Data Centre is used, which is limited in

capacity for ongoing operations. In order to address this challenge, a separate Server will soon be procured for which tender process has already been initiated.

The management's reply was not convincing as documentary evidence regarding initiatives taken by the department for the acquisition of a separate server for EMIS was not provided to audit.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the management to shift Database, Application, and Web Server onto separate servers to mitigate security, performance, data integrity risks.

4.3.4 Absence of Formal IT Assets Management Process	**Medium**

Pakistan National Cyber Security Policy 2021, (Clause 3.4.1) (Protection and Resilience of National Critical Information Infrastructure) recommends a culture of "accountability" and "self-governance" in respective public and private organizations will be responsible to safeguard their digital assets, data, products, and services to improve their confidentiality, integrity, and availability.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the entity did not have a formal process for identifying, labeling, and tracking IT assets, including hardware, software, and data.

This lack of control and oversight creates an environment where IT assets can be easily lost, stolen, or compromised lead to financial losses, business disruption, and reputational damage.

When pointed out by Audit in July 2024, the management stated that "as already mentioned above that IT/EMIS section is an integral part of E&SE Department and the Care Taker of E&SE Department looks after the assets of all kinds and provides maintenance facility. Also, in the iEMIS, there is a separate module for

Assets MIS for all the attached offices to enter and maintain records of all kind of equipment including IT equipment."

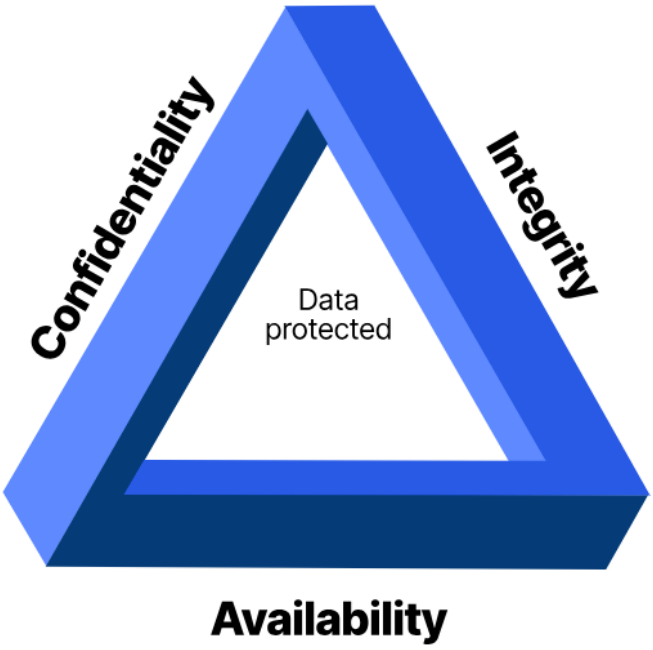
The management's reply was not convincing as the entity failed to produce documentary evidences in support of existence of a Formal IT Assets Management Process.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends that the organization should develop and implement comprehensive IT assets identification and classification policy and procedures that include clear definitions of IT assets and their classification categories, established procedures for identifying, labeling, and tracking IT assets, and defined roles and responsibilities for IT assets management.

4.4 INFORMATION SECURITY

Information Security is a critical component of an organization's overall security posture, encompassing the processes, technologies, and policies designed to protect sensitive information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It ensures the confidentiality, integrity, and availability of data, as well as authentication, authorization, and non-repudiation. Effective Information Security involves risk management, vulnerability assessment, threat analysis, incident response, security awareness training, and compliance with regulations and standards. By implementing robust Information Security measures, organizations can protect their assets, maintain trust and confidence, and ensure business continuity. This includes safeguarding personal data, financial information, intellectual property, and other sensitive data, as well as ensuring the security of systems, networks, and applications. By prioritizing Information Security, organizations can mitigate the risk of cyber threats, data breaches, and other security incidents, and ensure the long-term success and reputation of their organization.



(The 3 Principles of Information Security)

4.4.1 Absence of Formal User Access Management	High

Pakistan National Cyber Security Policy 2021, (Clause 3.5) states that "access to all government systems with the mandated and desired access control technology".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not have a formal user access management process in place. Access rights were not consistently granted, revoked, or reviewed, and there was no clear documentation of user roles and responsibilities.

This condition poses a significant risk to the organization, as unauthorized access to systems and data could result in data breaches, fraud, or disruption of services. Additionally, non-compliance with regulatory requirements may lead to legal and reputational consequences.

When pointed out by Audit in July 2024, the management stated that "SOPs and roles/ responsibility matrix for iEMIS is there and have been shared with the IS Audit team which clearly shows the roles and access provided to the users. Also, a review of access rights is done by the EMIS and after deliberation new rights are given or taken back."

The management's reply was not tenable as formal user access management processes were not in place. No documents regarding a formal User Access Management were provided in support of reply.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the management to develop and implement a comprehensive user access management policy and conduct a thorough review of current access rights to revoke unnecessary access and consider implementing an Identity and Access Management (IAM) system, and maintain accurate records of access rights.

4.4.2 Excessive SUPER ADMIN Accounts and Misuse of Privileges	High

ISO 27001, ACCESS CONTROL, Section A.9.1.1, requires that "an access control policy shall be established, documented and reviewed based on business and information security requirements".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that there was disproportionately high number of user accounts with SUPER ADMIN (administrator-level) access, totaling 42 accounts (Appendix IS-02). It was further noted that many of these SUPER ADMIN accounts were assigned to non-administrative personnel who were using these privileges i.e. adding a new user, enhancing or limiting users' authorization and deleting user etc. from the system for routine application access. This practice violates the principle of least privilege, as these accounts had unrestricted access to sensitive data and critical system configurations, posing significant security risks.

This condition poses a significant risk to the organization as it allows unauthorized access to sensitive data and changes to system configurations may be made without proper authorization or tracking. It increases the risk of data breaches and cyber-attacks.

When pointed out by Audit in July 2024, the management stated that "all users of iEMIS have already been defined according to the recommendations. However, the same will be revisited again to ensure accuracy and completeness."

The management's reply was inadequate as the department did not establish and document an access control policy based on business and information security requirements. No documentary proofs were provided in support of reply.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends that the organization should take immediate action to revoke administrative privileges from non-administrator personnel and create individual user accounts for all personnel, with appropriate roles and permissions.

4.4.3 Lack of Regular User Account Review and Recertification	Medium

Pakistan National Cyber Security Policy 2021, (Clause 3.5) states that “access to all government systems shall be with the mandated and desired access control technology”.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not conduct regular reviews and recertification of user accounts, including privileged accounts and accounts with elevated access levels.

This lack of review lead to inactive accounts remaining active, potentially allowing unauthorized access. Privileged accounts being misused or compromised without detection and elevated access levels being granted unnecessarily, increasing the attack surface.

When pointed out by Audit in July 2024, the management stated that monthly data updation and submission of online certificate process have been initiated for each user and is verified during the first week of each month. If a user fails to comply, then the necessary administrative measures are suggested to the Department management.

The management's response was insufficient as no documentary proofs regarding regular review and recertification of user accounts were provided to audit.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to establish a formal user account recertification process to ensure regular review and validation of active user accounts. Implement a procedure to timely identify and remove dormant accounts.

4.4.4 Weak Password and Session Controls	High

Pakistan National Cyber Security Policy 2021, (Clause 3.5) mandates to define and enforce a robust Government Authentication and Data Protection Framework including data classification and to ensure that appropriate controls exist to protect data.

During IS audit iEMIS for the Audit Year 2023-24, it was observed that the organization did not have a strong password policy in place which means that;

i. Passwords were not complex meaning thereby having both alpha and numeric values, case-sensitive, different characters etc.
ii. Passwords were not changed regularly (e.g. every 60 - 90 days)
iii. Users account were not locked after 5-6 invalid attempts
iv. No restriction on password history, users are reusing the same passwords repeatedly.

Risks of having no strong password policy include weak passwords being easily guessed or cracked, leading to unauthorized access and potential security breaches. This can result in data theft, financial losses, reputation damage, and compliance risks, emphasizing the need for a robust password policy.

When pointed out by Audit in July 2024, the management stated that “the iEMIS already follows standard password (minimum 8 character consisting of numbers, alphabets or special characters) rules. However, with over 35,000 users, many of them are not IT literate; there have been numerous issues with regularly changing passwords. In light of the recommendations, a mechanism will be devised to ensure password security and data integrity while addressing these challenges.”

The management's reply was not satisfactory as there were no multi-factor authentication, password rotation and account lockout policies. No documentary proofs were provided regarding the existence of appropriate controls to protect data.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to develop and enforce a strong password policy with minimum length, complexity, and regular changes, and consider implementing a password manager. Enable multi-factor authentication and conduct regular password audits to ensure secure password practices.

4.4.5 Lack of Standard System Baseline Configuration	High

ISO 27001, (OPERATIONS SECURITY), (Clause A.12.1.1) mandates “ensuring correct and secure operations of information processing facilities by documentation of operating procedures”.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not document the standard system baseline configuration. Baseline configurations provide a reference point for system builds, releases, and changes. Without them, the organization lacks a basis for ensuring IT consistency and security. The absence of a baseline configuration hinders the ability to effectively manage, secure, and audit the IT infrastructure.

In secured Operating System configurations exposed the organization to security risks, including unauthorized access and malicious activity. Inconsistent configurations also lead to operational inefficiencies, compliance issues, and increased maintenance costs.

When pointed out by Audit in July 2024, the management stated that “these recommendations are noted and will be implemented following the completion of the previously mentioned recommendations and the development of a comprehensive IT Digital Policy and Strategy.”

The management's reply was not convincing as no specific timeline for documentation of standard system baseline configuration and development of IT Digital Policy for the department was shown to audit till finalization of the report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends to develop, document, and implement a standardized baseline configurations for all critical IT systems, including Operating Systems, databases, web servers, and network appliances. Conduct regular audits to verify compliance with the established baseline, identifying and remediating any deviations or vulnerabilities.

4.4.6 Absence of Encryption for Sensitive Data Transmission	High

ISO 27001, (COMPLIANCE), (Clause A.18.1.3) requires that "information shall be protected from loss, destruction, falsification and unauthorized access in accordance with legislator, regulatory, contractual and business requirements".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization's web application transmitted sensitive data in plain text, without encryption, and did not utilize Secure Socket Layer (SSL), (Appendix IS-3) which is a cryptographic protocol used to authenticate internet connection and enable the encryption and decryption for secure network communication. This will expose sensitive information, such as student records, personal data, and authentication credentials, to potential interception and unauthorized access, posing significant security risks.

The transmission of web application data in unencrypted format and the lack of Secure Socket Layer (SSL) implementation poses a significant risk to the confidentiality, integrity, and security of sensitive data. This vulnerability allows unauthorized parties to intercept and access sensitive information, such as user credentials, and personal data.

When pointed out by Audit in July 2024, the management stated that "the iEMIS is currently accessible via an IP address, and proper domain name has not been assigned yet. The process of assigning a proper domain name will be initiated and will soon ensure the installation of an SSL certificate as well."

The management's response was inadequate as no documentary evidences regarding the installation and utilization of SSL certificate to protect the risk of confidentiality and integrity of data were provided to Audit Team.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends entity to implement Secure Socket Layer (SSL) to encrypt web application data in transit, protecting sensitive information from interception and unauthorized access. Configure the web server to use HTTPS protocol and ensure SSL certificates are properly installed and configured to secure data transmission.

4.4.7 Oracle Database Port Publicly Accessible	**High**

ISO 27001, (ACCESS CONTROL), (Clause A.9.2.3) requires that "the allocation and use of privileged access rights shall be restricted and controlled".

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the few critical ports, including Oracle database default port (1521) and another unknown port (8085) was open and accessible to the public internet (Appendix IS-4), which clearly shows that the ports being open and accessible publicly can be hacked easily by an unauthorized person. This configuration exposes the database to potential unauthorized access and various security threats, including brute force attacks, SQL injection, and data breaches.

Allowing critical system ports opened and accessible to the public internet increases risk of unauthorized access, data breaches, SQL injection, reputation damage, and non-compliance to regulatory requirements.

When pointed out by Audit in July 2024, the management stated that "iEMIS has already restricted all the ports, allowing only the necessary ones. However, in pursuance of the recommendations, all the ports will be revisited / reviewed their configurations to ensure they meet current security standards."

The management's reply was not satisfactory as most of the sensitive ports were found opened to public domain. No documentary proofs in support of reply or any progress in the matter was shown to audit.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to urgently restrict public access to the Oracle database port (1521). Additionally, a comprehensive assessment should be conducted on all open ports to identify potential vulnerabilities and ensure that only necessary ports remain accessible.

4.4.8 Insufficient Authentication Mechanism	High

Pakistan National Cyber Security Policy 2021, (Clause 3.5) mandates to define and enforce a robust Government Authentication and Data Protection Framework including data classification and to ensure that appropriate controls exist to protect data.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization was using single factor authentication (SFA) to secure access to sensitive data and systems. SFA relies on only one factor authentication level, such as a password or username, to verify the identity of users.

Access rights are based on roles and responsibilities and are predefined for each position. This approach of having reliance only on SFA poses a significant threat to the organization's security or data as SFA does not provide protection against unauthorized access.

When pointed out by Audit in July 2024, the management stated that “the users of iEMIS are very diverse in nature and belong to different background and IT skills. To facilitate all kind of users multifactor authentication has not been implemented. But this department believes in strong security and shall implement multifactor authentication in future.”

The management agreed with audit’s stance. However, the documentary proofs for shift towards implementation of multifactor authentication to ensure the security and integrity of the iEMIS, were not provided in support of reply.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the entity to document and justify excess rights for all users, and implement a role-based access control model to ensure least privilege access. Implement multi-factor authentication to strengthen security and prevent unauthorized access.

4.4.9 Absence of performing Regular Penetration Testing	**Medium**

Pakistan National Cyber Security Policy 2021, (Clause 3.6) mandates to create infrastructure and/or leverage existing facilities/ platforms/ resources for conformity assessment and certification of compliance to Cyber Security best practices, standards, and guidelines (e.g., ISO 27001 ISMS certification or other industry standards and benchmarks, internal security system audits, Penetration testing / vulnerability assessment, application security testing, web security testing, business continuity planning test, etc.).

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization never performed penetration testing on its network or application, which means that potential security vulnerabilities and weaknesses remain unidentified and unaddressed.

The absence of penetration testing on the network or application poses a significant risk, as it leaves vulnerabilities undetected and un-remediated, potentially allowing unauthorized access, data breaches, and malicious activities to occur, compromising the confidentiality, integrity, and availability of sensitive data and systems.

When pointed out by Audit in July 2024, the management stated that penetration testing and Quality Assurance needs special expertise and the present IT/EMIS team lacks that expertise. For compliance of the recommendations, either the KP IT Board will be approached or services of third party will be hired which will definitely involve availability of resources/budget.

The management reply was not satisfactory as the evidence for approaching Khyber Pakhtunkhwa IT Board or hiring the services of third party for penetration testing and demand for additional budget were not shown to audit.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends the management to conduct regular penetration testing (at least annually) to identify vulnerabilities and weaknesses in the network and application.

4.4.10 Weak Physical and Environmental Controls in Datacenter	**Medium**

ISO 27001, (Physical and Environmental Security), (Clause A.11.1.1) states that security perimeters shall be defined and used to protect areas that contain both sensitive or critical information and information processing facilities.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, the audit of the data center (physical examination) revealed significant security and safety risks. The use of single-factor authentication via access cards for entry poses a substantial security risk, as it can be easily compromised. Furthermore, the absence of entry logs prevents tracking and monitoring of individuals entering the facility, compromising data and equipment security. The data center's construction using non-fireproof materials also poses a significant fire safety risk.

Other notable risks include the lack of regular maintenance records for smoke detection alarms, the use of glass doors that can be easily broken, and the absence of a water detection and removal mechanism, leaving the facility vulnerable to water damage and potential data loss. These findings highlight the need for enhanced security measures, including multi-factor authentication, reinforced doors and walls, regular maintenance of critical systems, and a comprehensive water management system. Audit apprehends that the existing vulnerabilities could be exploited by a potential incident, leading to a catastrophic event of significant magnitude.

When pointed out by Audit in July 2024, the management stated that these recommendations pertain to KP Data Centre and the Audit team is requested to share the same with KP Data Centre for their views/inputs accordingly.

The management’s reply was not convincing as it was the responsibility of the E&SE Department KP to get comments from the Data Center. No progress was shown till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends that the organization should enhance the data center's security and safety, implement multi-factor authentication, including biometric scanners or smart cards, and maintain accurate entry logs. Additionally, a seismic assessment should be conducted, non-fireproof materials should be replaced with fire-resistant ones, and regular maintenance schedules established for smoke detection alarms to ensure compliance with fire safety standards and overall stability and safety of the data center.

4.5 BUSINESS CONTINUITY AND RISK MANAGEMENT

Business Continuity and Risk Management is a comprehensive approach that enables organizations to identify, assess, and mitigate potential risks that could disrupt their operations, while also ensuring the continuity of critical business functions during unexpected events or disasters. It involves identifying and assessing potential risks, developing strategies to mitigate or manage them, and implementing plans to ensure business continuity, such as backup systems, emergency response plans, and disaster recovery procedures. By proactively managing risks and ensuring business continuity, organizations can minimize the impact of disruptions, protect their reputation, and ensure the continued delivery of products and services to their customers, ultimately contributing to their long-term success and sustainability.

Business Continuity Life Cycle

4.5.1 Absence of Business Continuity and Disaster Recovery Plan	High

ISO 27001, (Information Security Aspects of Business Continuity Management), (Clause A.17.1.2) mandates that "the organization shall establish, document, implement and maintain processes, procedure and controls to ensure the required level of continuity for information security in adverse situation (e.g during crisis or disaster)". Figure 33—COBIT 5 (Roles and Organizational Structure), defines that an individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, shall ensure that the enterprise's critical functions continue to operate disruptive events.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not have a Business Continuity Plan (BCP) and Data Disaster Recovery Plan (DRP) in place. Additionally, there is no disaster recovery offsite, nor are offsite backups maintained. This lack of formalized plans leaves the organization highly vulnerable to potential disruptions and disasters, posing significant risks to operational continuity and data integrity

The absence of a BCP and DRP poses significant risks to the organization, including disruption of critical business functions and operations, data losses and corruption, reputational damage and loss of customer trust, financial losses and legal liabilities and Non-compliance with regulatory requirements.

When pointed out by Audit in July 2024, the management stated that "the KP Data Center has already informed the Audit Team in online meeting that a Backup site is in place and in case any emergency arises, data can be recovered. Secondly this IT/EMIS section of E&SE Department also regularly takes backup of the system and stores in offline media for disaster recovery."

The management's response was not convincing as no proofs for existence of documented robust BC/DR plans were provided to audit till finalization of this report.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

Audit recommends that entity should conduct a business impact analysis to identify critical functions and define Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

4.5.2 Absence of Formal Process for Managing Tapes and Removable Media	Medium

Pakistan National Cyber Security Policy 2021, (Clause 3.4) (Protection and Resilience of National Critical Information Infrastructure), recommends a culture of "accountability" and "self-governance" in respective public and private organizations will be responsible to safeguard their digital assets, data, products, and services to improve their confidentiality, integrity, and availability.

During IS audit of the iEMIS of Elementary & Secondary Education Department Khyber Pakhtunkhwa, Peshawar for the Audit Year 2023-24, it was observed that the organization did not have a formal process for managing tapes and removable media, including regular inventory and tracking, secure storage and handling, and defined retention and disposal policies.

Without a tapes/removable media management procedure, the organization is at risk of data loss, theft, or unauthorized access, which can lead to business disruption and reputational damage. Furthermore, non-compliance with regulatory requirements can result in legal consequences.

When pointed out by Audit in July 2024, the management stated that "these recommendations are noted and will also be implemented following the completion of the previously mentioned recommendations and the development of a comprehensive IT Digital Policy and Strategy."

The management agreed to audit's stance.

PAO (Secretary Education KP) was requested to convene DAC meeting in August 2024 with subsequent reminders, which could not be convened till finalization of this report.

The audit recommends that organization should develop and implement a comprehensive tapes/ removable media management policy and procedure that includes regular inventory and tracking, secure storage and handling, defined retention and disposal policies, and compliance with regulatory requirements.

ACKNOWLEDGEMENT

Audit would like to take this opportunity to thank Elementary & Secondary Education Department, Government of Khyber Pakhtunkhwa Peshawar for their cooperation and assistance during the course of this audit.

Appendix IS-1 (Terms of Reference)

TERMS OF REFERENCE (TOR) FOR INFORMATION SYSTEM AUDIT OF INTEGRATED EDUCATION MANAGEMENT INFORMATION SYSTEM ELEMENTARY & SECONDARY EDUCATION DEPARTMENT GOVERNMENT OF KHYBER PAKHTUNKHWA

1. INTRODUCTION

Elementary & Secondary Education Department (E&SED) Khyber Pakhtunkhwa using Integrated Education Management Information System iEMIS for record keeping. EMIS Cell of E&SED has developed an integrated Education Management Information System (iEMIS) based on the Software Requirement Specification (SRS) for key systems within E&SED under Khyber Pakhtunkhwa Education Improvement Program (KPEIP) funded through Education Sector Program Implementation Grant (ESPIG) of Global Partnership for Education (GPE). The SRS document has been approved by E&SED as a living document in January 2023. As part of roadmap of SRS document and phase wise implementation plan of the iEMIS, it is imperative to initiative implementation of prioritized systems within E&SED. For this purpose, EMIS cell has developed operational plan, as well as concept paper proposing to strategize and align E&SED's structure from Provincial to SDEO levels for effective rollout, implementation and use of iEMIS.

2. OBJECTIVES

The primary objectives of the Information System audit of iEMIS are:

- To check the IT Governance for effective management of software ensuring alignment with educational objectives, efficient resource management
- To evaluate the process of Information Systems development, acquisition and Implementation for ensuring the formal software development lifecycle, quality assurance, and controlling configuration changes
- To check the adherence of information system outsourcing and operations with applicable laws, regulations, and international established best practices
- To examine the information security system, its robustness, reliability of the IS infrastructure,
- To examine maintenance & support system
- To check the business continuity plan and disaster recovery plan.

3. SCOPE

The scope of the IS audit will include but not be limited to:

General Computer Controls (GCC) Review:

- Information Technology Governance.
- Information Systems Development, Acquisition and Implementation
- Information Systems Security.
- Information Systems Outsourcing.
- Information Systems Operations, Maintenance & Support
- Business Continuity Plan & Disaster Recovery Plan

4. METHODOLOGY

The IS audit will be conducted in accordance with the related laws and regulations, International Standards of Auditing applicable in auditing government sector, and best practices, including:

- Conduct interviews with key stakeholders, including IT management, system administrators, security personnel, and other relevant parties, to gain a comprehensive understanding of the organization's security posture, practices, concerns and potential area of improvement.
- Examine and analyze relevant documentation, including IS policies, procedures, risk assessments, incident reports, and other supporting records.
- Conduct comprehensive technical testing, including vulnerability scanning, penetration testing, and configuration reviews, to identify potential security weaknesses, assess the effectiveness of existing controls, and provide actionable recommendations for remediation and improvement.
- Analysis of system logs and audit trails to identify potential security incidents, track user activity, and monitor system behavior.
- On-field physical inspections of IS infrastructure and available facilities.

5. TIMELINE

The IS audit will be conducted w.e.f. 15th April, 2024 to 31st May, 2024, as per following schedule.

Planning and Preparation	15.04.2024 to 28.04.2024
Fieldwork and Execution	29.04.2024 to 07.06.2024
Reporting and Presentation	07.06.2024 to 26.07.2024

6. DELIVERABLE

The following will be the outcomes upon completion of this IS audit:

- *IS Audit Report:* A thorough and detailed document presenting the audit's key findings, observations, and actionable recommendations, providing a clear and concise overview of the audit's outcomes and guidance for improvement.
- *Executive Summary:* A summary of the key audit findings and recommendations for the management.
- *Management Presentation:* A presentation to senior management highlighting the audit results, implications, and proposed remediation actions.

7. REPORTING

The IS audit findings will be reported to the Director General Audit (Local Government), Khyber Pakhtunkhwa and senior management of the entity. The audit report will also be shared with relevant stakeholders, including IT management and the top-level management.

8. QUALITY ASSURANCE

The IS audit will adhere to internationally recognized standards and best practices, including INTOSAI GUID 5100 on audit of Information Systems, ISACA's COBIT framework and the Institute of Internal Auditors (IIA) standards. Quality assurance measures will be implemented throughout the audit process to ensure the accuracy, reliability, and objectivity of the findings.

9. CONFIDENTIALITY

The IS audit team will maintain the confidentiality of all information obtained during the audit, disclosing it only to authorized personnel on a need-to-know basis. The team will strictly adhere to robust confidentiality protocols, protecting the sensitive information and privacy of the auditee organization and upholding the highest standards of professional conduct.

10. INDEPENDENCE

The IS audit team will uphold independence and objectivity throughout the audit process, ensuring an unbiased and impartial assessment. Any potential conflicts of interest will be proactively identified and managed in accordance with established protocols, guaranteeing the integrity, reliability, and credibility of the audit findings.

11. RESOURCE

The IS audit team will be staffed by qualified and experienced auditors with in-depth knowledge of information systems, cyber-security, and audit best practices, enabling a rigorous and effective evaluation. The team will have access to ample resources, including specialized personnel, tools, and innovative technology, to ensure a successful and comprehensive audit outcome.

1.	Mr. Sajid Khan	Director Audit, O/o the DGA Local Govt. KP (Team Leader)
2.	Mr.Yaser Fadil	CIPFA Consultant
3.	Mr. Artan Osman	CIPFA Consultant
4.	Mr. Sahibzada Waheed	Audit Officer, O/o the DGA Local Govt KP, Peshawar
5.	Mr. Khurram Shahzad	Audit Officer, O/o the DGA Social Safety Net, Islamabad
6.	Mr. Tauseef Khalid	Senior Auditor, O/o the DGA P&NR, Islamabad.

12. AMENDMENTS

Any amendment or changes to these Terms of Reference shall be approved by the Auditor General of Pakistan and communicated to all relevant stakeholders.

13. APPROVAL

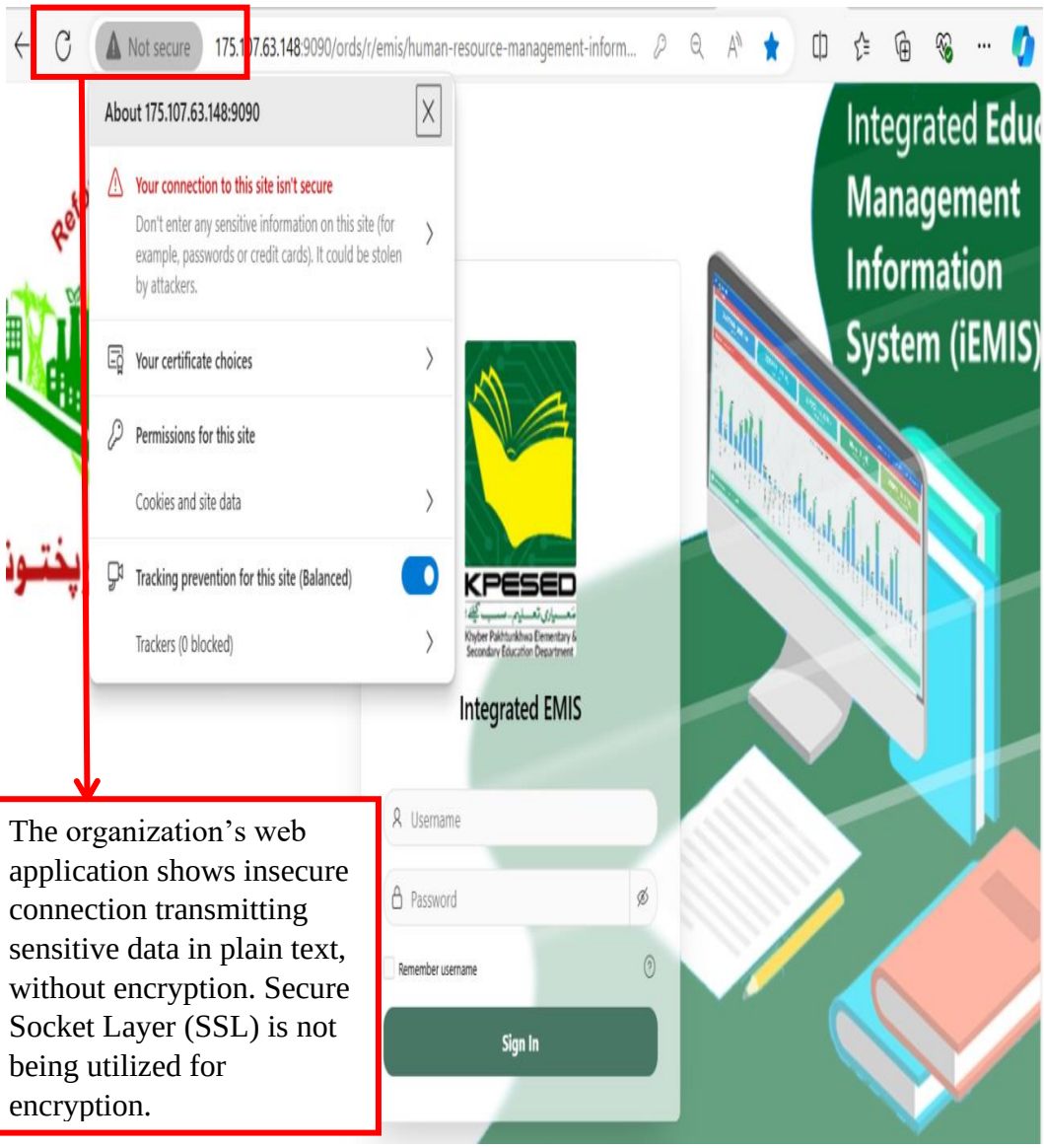
These Terms of Reference for the Information System (IS) Audit of iEMIS E&SE Department Khyber Pakhtunkhwa are hereby approved by the Auditor General of Pakistan on .04.2024

Appendix IS-2 (Excessive Use of Super Admin Accounts and Misuse of Privileges)

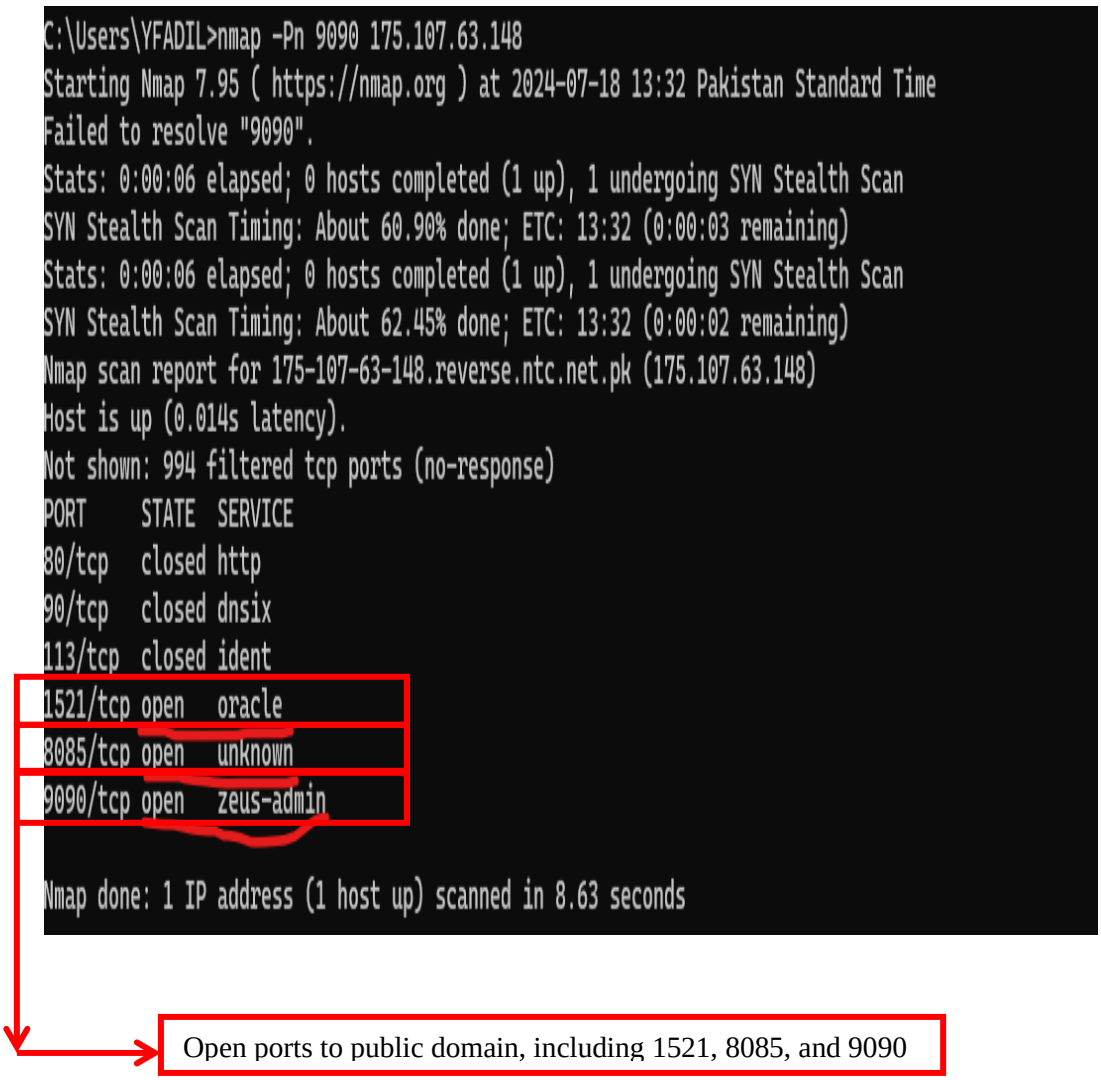
List of user accounts with SUPER ADMIN privilege, totaling 42 accounts.

USERNAME	Group_Name	USER_STATUS	ADMIN_TYPE	ADMIN_NAME
SOMANAGEMENT	SO School	A	SA	SUPER ADMIN
HAMZARAUF	PEMIS	A	SA	SUPER ADMIN
ATIFIQBAL	PEMIS	A	SA	SUPER ADMIN
PSRA_ADMIN	PSRA ADMIN	A	SA	SUPER ADMIN
MAGORAKZIA	PEMIS	A	SA	SUPER ADMIN
ESED	COVID GROUP	A	SA	SUPER ADMIN
SECRETARY	Secretary Group	A	SA	SUPER ADMIN
GHANIAKBARPEMIS	ADMINISTRATOR	A	SA	SUPER ADMIN
RNIESED	RNI ESED	A	SA	SUPER ADMIN
FAYAZUDDINAFRIDI	Secretary Group	A	SA	SUPER ADMIN
KASHIFPEMIS	ADMINISTRATOR	A	SA	SUPER ADMIN
EMA_ADMIN	EMA ADMIN	A	SA	SUPER ADMIN
SAJIDKHANPEMIS	ADMINISTRATOR	A	SA	SUPER ADMIN
TEXTBOOKBOARD	Textbook Board	A	SA	SUPER ADMIN
PROJECTS	RNI PROJECTS	A	SA	SUPER ADMIN
SOMALE	SO School	A	SA	SUPER ADMIN
SOFEMALE	SO School	A	SA	SUPER ADMIN
DIREMIS	PEMIS	A	SA	SUPER ADMIN
SUPERADMIN	ADMINISTRATOR	A	SA	SUPER ADMIN
DDEMIS	PEMIS	A	SA	SUPER ADMIN
HUSSAIN	ADMINISTRATOR	A	SA	SUPER ADMIN
AZIZPEMIS	PEMIS	A	SA	SUPER ADMIN
SMAGO	ADMINISTRATOR	A	SA	SUPER ADMIN
SPO1	P&D Admin	A	SA	SUPER ADMIN
ZAINULLAH	PEMIS	A	SA	SUPER ADMIN
SOPRIMARYFEMALE	SO Primary	A	SA	SUPER ADMIN
GUEST_UNICEF	Guest_UNICEF	A	SA	SUPER ADMIN
SSRMONITORING	SSR Monitoring	A	SA	SUPER ADMIN
DIRECTOREMIS	PEMIS	A	SA	SUPER ADMIN
ADIL.PEMIS	ADMINISTRATOR	A	SA	SUPER ADMIN
GUEST	Secretary Group	A	SA	SUPER ADMIN
DSBUDGET	Secretary Group	A	SA	SUPER ADMIN
SOPRIMARYMALE	SO Primary	A	SA	SUPER ADMIN
CAR	CAR (Afghan Commissionerate) Admin	A	SA	SUPER ADMIN
AZAZ.PEMIS	ADMINISTRATOR	A	SA	SUPER ADMIN
FINANCEDEPT	finance department	A	SA	SUPER ADMIN
SOACCOUNTS	Accounts	A	SA	SUPER ADMIN
WISAL.PEMIS	SO School	A	SA	SUPER ADMIN
GHANI	Secretary Group	A	SA	SUPER ADMIN
SOG	SO General	A	SA	SUPER ADMIN
MALAM	P&D Admin	A	SA	SUPER ADMIN
ZAHID.PEMIS	SO School	A	SA	SUPER ADMIN

Appendix IS-3: Absence of Encryption for Sensitive Data Transmission
Failure to implemented SSL will expose sensitive information, such as student records, personal data, and authentication credentials, to potential interception and unauthorized access, posing significant security risks.



Appendix IS-4: Ports Accessible Publically



Appendix IS-R: Exceptions Rating Matrix

High	Action plan and related corrective action to be implemented as a matter of urgency.
Medium	Action plan and related corrective action to be implemented as a matter of priority.
Low	Action to be taken to address weakness within a reasonable agreed time frame.
Improvement Opportunity	Action to be taken to improve effectiveness of a control based on agreed best practices.

System Efficiency (Automated vs Manual)	1. Fully Automated (No manual processes) 2. Highly Automated (Some manual processes) 3. Equally relied (50% Automated, 50% Manual) 4. Highly Manual (Some Automated processes) 5. Fully Manual (No automated processes)
IT Governance	1. Excellent 2. Very Good 3. Good 4. Fair 5. Poor
Service Delivery	1. Very Satisfied 2. Satisfied 3. Neutral 4. Dissatisfied **5.** Very Dissatisfied