Audit Report

For

BAZY TRADING & CONTRACTING CO. LTD

Stage 2

Audit Dates: 28/09/2025 to 30/09/2025

Organization Details

Company:	BAZY TRADING & CONTRACTING CO. LTD
Address:	Atiyah Al Fadani Street, Salauddin Al Ayoubi Road, Malaz, Riyadh, Saudi Arabia
Contact Person:	Eng. Tarek Saleh
Email:	info@bazy.com.sa
Audit Criteria:	ISO 27001:2013 / ISO 20000:2018
EA Code:	-
Scope:	ICT systems integrator and services provider across the MENA region
No. of Sites:	1

Sites

Site Name	Location
SAME SITE	SAME LOCATION

Audit Objectives

Audit Objectives: To determine conformity of the management system, or parts of it with audit criteria and its:
- ability to ensure applicable statutory, regulatory and contractual requirements are met,
- effectiveness to ensure the client can reasonably expect to achieve specified objectives

and to identify as applicable areas for potential improvement.

Auditors

Auditor Name	Role
Eng. Adel Belal	Lead Auditor
Eng. Ali Bedawy	Auditor
Eng. Hussien Fawzy	EGAC Observer

Auditee Members

Auditee Name	Position
Tarek Saleh	IT Manager

Shadi Al-Tamimi	Bazy Top Managment Representative _IT Group Manager
Ahmed Barghout	QHSE Mnanger
Nasser Mansuor	HR Manager
Khaled Younes	Admin Supervisor
Essam Mohamed	SD Manager

No. of Man-Days
5.5

Audit Findings

Clause No.	Requirement\\Departement	Evidence	Result
4.1	check internal and external issues considering climate changes	Sample taken for Internal issues : - Lack of awarness (-ive) - using of Trio-Application (+Ive) - leadership commitment (+Ive) - Known limitations (-ive) Sample taken for external issues: - Technology changes (-ive) - Changes in Security laws(-ive) - Free Information Security Governamental services (+ive). - Market competetion (-ive) - Climate Changes (-ive) Documented in XLS sheet for Bazy Issue Register	OK
4.2	Check intereasted parties and their requirements including which of these requirements cosidered as legal requirements or SLAs (service level agreements)	Sample for Interested parties and their requirements: 1. National Cybersecurity Authority (NCA) Law Name: Cybersecurity Governance Framework (2020) Law Number: N/A (Issued as a framework). Requirements: Implement security controls (encryption, secure access). Perform regular risk assessments and audits. Establish incident response plans for cyber breaches. Ensure governance of cybersecurity roles	OK

Clause No.	Requirement\\Departement	Evidence	Result
		and responsibilities. Law Name: National Cybersecurity Strategy Law Number: N/A. Requirements: Develop organizational cybersecurity policies. Share threat intelligence between public and private sectors. Train and educate staff on cybersecurity awareness. Use local cybersecurity technologies and expertise. 2. Saudi Data & Artificial Intelligence Authority (SDAIA) Law Name: Personal Data Protection Law (PDPL, 2021) Law Number: Royal Decree No. M/19 (Dated 09/02/1443H). Requirements: Obtain explicit consent before collecting or processing personal data. Data must only be used for the stated purpose. Enable individuals to access, modify, or delete their personal data. Prohibit cross-border data transfers without approval. Keep personal data secure with encryption and access controls. 3. Ministry of Communications and Information Technology (MCIT) Law Name: Electronic Transactions Law (2007) Law Number: Royal Decree No. M/18 (Dated 08/03/1428H). Requirements: Ensure the authenticity and integrity of electronic records. Use secure electronic signatures. Protect sensitive data in electronic transactions. Provide legal recognition to electronic contracts and communications. Law Name: E-Commerce Law (2019) Law Number: Royal Decree No. M/126 (Dated 07/11/1440H). Requirements:	

Clause No.	Requirement\\Departement	Evidence	Result
		Protect consumer data in e-commerce transactions. Use secure payment systems. Clearly display terms of sale, return policies, and warranties. Maintain the confidentiality of customer information. 4. Communications and Information Technology Commission (CITC) Law Name: Cloud Computing Regulatory Framework (2018) Law Number: N/A (Issued by CITC). Requirements: Protect customer data stored in cloud systems. Restrict cross-border data transfers without approval. Implement robust cybersecurity measures (e.g., backup and disaster recovery). Notify customers of data breaches. Law Name: IoT Regulatory Framework (2020) Law Number: N/A (Issued by CITC). Requirements: Secure IoT devices and networks. Ensure data privacy and protection in IoT systems. Comply with cybersecurity standards for IoT devices. 5. Bureau of Experts at the Council of Ministers Law Name: Anti-Cybercrime Law (2007) Law Number: Royal Decree No. M/17 (Dated 08/03/1428H). Requirements: Prohibit unauthorized access to IT systems. Criminalize data theft, alteration, or destruction. Penalize electronic fraud and identity theft. Enforce penalties for cyber defamation and blackmail. Imprisonment and fines for offenders (up to SAR 5 million or 10 years). 6. Saudi Authority for Intellectual Property (SAIP) Law Name: Copyright Law (2020 Amendment)	

Clause No.	Requirement\\Departement	Evidence	Result
		Law Number: Royal Decree No. M/41 (Dated 02/07/1424H). Requirements: Protect digital intellectual property, including software and databases. Enforce penalties for copyright infringement. Register copyrights with SAIP for legal protection. Law Name: Patent Law Law Number: Royal Decree No. M/27 (Dated 29/05/1425H). Requirements: Protect cybersecurity-related innovations, such as software or devices. Prevent unauthorized use or copying of patented technologies. 7. General Authority for Statistics (GASTAT) Law Name: Statistics Law Law Number: Royal Decree No. M/90 (Dated 06/09/1437H). Requirements: Protect statistical data confidentiality. Secure data collection, processing, and storage processes. Prohibit unauthorized disclosure of individual or organizational data. 8. Ministry of Interior Law Name: Combating Information Crimes Law Law Number: N/A (Under Ministry of Interior guidelines). Requirements: Prevent misuse of IT systems for malicious purposes. Penalize activities like hacking, phishing, and malware distribution. Coordinate with local and international bodies for cybercrime investigations.	
4.3	Organization documented scope	Same as Stage 1 no change.	OK

Clause No.	Requirement\\Departement	Evidence	Result
4.4	Service & Information security management systems including main service proceses and their interactions between them.	- Description for datacenter system topology which accessed by IT manager only (A8.27 Secure system architecture and engineering principles) as follows: start with two routers one for STC and the other for ..... and temperary 5G wireless router for emergency use only , these routers connected directely to two redundancy (A8.14 Redundancy of information processing facilities) firewall which have web filter control (A8.23 Web filtering) and (A8.7 Protection against malware) protection against viruses and configured (A8.9 Configuration management) to disable for suspected IPs for restricted access (A8.3 Information access restriction) applied through following access policy control (A5.15 Access control) then connected directly to a core switch working redundncy by another backup switch not connected but available in cabient as standby shall be connected within 15 min.(A8.14 Redundancy of information processing facilities) . then switch is connected directly to batch panel in the network (passive) cabinet. the batch panel connnected to server cabient batch panel which connected to three severs as follows: 1) Host Processor: Intel Xeon Processor D- Host Memory: 16 GB DDR4 Host Storage: 4 TB RAID 5 Host OS: VMware Host Application: APPSHARE SERVER VM Name: ICC Hostname / Server Name: 172.16.1.1 Virtual Machines: 3 CPU: 4 RAM: 8 GB Storage: 1 TB Host Storage Remaining: 3 TB 2) Host Processor: Intel Xeon Processor D- Host Memory: 32 GB DDR4 Host Storage: 6 TB RAID 5 Host OS: VMware	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Host Application: Backup/Archiving (Acting Backup Host) VM Name: BACKUP Hostname / Server Name: 172.16.1.2 Virtual Machines: 4 CPU: 8 RAM: 16 GB Storage: 2 TB Host Storage Remaining: 4 TB 3) Host Processor: Intel Xeon Processor D- Host Memory: 64 GB DDR4 Host Storage: 4 TB RAID 1 Host OS: Microsoft Hyper-V Host Application: TrendAV VM Name: TRENDAV Hostname / Server Name: 172.16.2.1 Virtual Machines: 2 CPU: 4 RAM: 32 GB Storage: 1 TB Host Storage Remaining: 3 TB 4) Host Processor: Intel Xeon Processor D- Host Memory: 16 GB DDR4 Host Storage: 8 TB RAID 6 Host OS: VMware Host Application: SQL (Primary SQL Server) VM Name: PRIMARYSQL Hostname / Server Name: 172.16.2.2 Virtual Machines: 5 CPU: 4 RAM: 16 GB Storage: 4 TB Host Storage Remaining: 4 TB 5) Host Processor: Intel Xeon Processor D- Host Memory: 32 GB DDR4 Host Storage: 8 TB RAID 6 Host OS: VMware Host Application: Veeam Server VM Name: VEEAMSERVER Hostname / Server Name: 172.16.2.3	

Clause No.	Requirement\\Departement	Evidence	Result
		Virtual Machines: 2 CPU: 8 RAM: 32 GB Storage: 4 TB Host Storage Remaining: 4 TB the core switch connected also directly to each floor switch. each floor have two switches one for connected PCs through access points and the other one connected IP phones network and PCs this network segregated from the other one also applied VLANs for each department in the floor (A8.22 Segregation of networks) and all network cables used are securly protected in the condut in the wall (A8.20 Networks security) the network cables are designed to ensure the service level agreements ahceivment (A8.21 Security of network services). Firewalls connected directly to UCM phones EXT (IP phone central). which connected to core switch.	

Clause No.	Requirement\\Departement	Evidence	Result
5.1	Leadership and commitment	- Integrated service & ISMS management policy and objectives are established. (See Stage 1 Report) - service management plan have been created (See Stage 1 Report) - Appropriate levels of authority are assigned for making decisions related to the SMS and the services; and this according to job desciption (5.3) and this also within defined risk managment and controlled Annex for A.5.2 Information security roles and responsibilities and with A5.3 Segregation of duties for segregating Conflicting duties and conflicting areas of responsibility , and A5.4 Management responsibilities for ensuring that all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization including authority for Contact with authorities (A5.5) specially for InfoSec related subjects - check availability of customer requirements have been determined through SLAs with STC , Nokia as samples for SLAs.	OK

Clause No.	Requirement\\Departement	Evidence	Result
5.3	Organizational roles, responsibilities and authorities	Check the following sample job descriptions : 1. IT Service Delivery Roles Service Delivery Manager : - Oversee end-to-end delivery of IT services. - Ensure compliance with SLAs (Service Level Agreements). - Manage client relationships and escalations. IT Project Manager: - Plan, execute, and monitor IT service-related projects. - Coordinate with teams for tower installations and infrastructure upgrades. Service Desk Manager : - Supervise IT support teams. - Ensure timely resolution of customer tickets. - Manage incident and problem management processes. IT Support Specialist : - Provide technical support to clients and internal teams. - Troubleshoot issues related to IT infrastructure and network connectivity. Network Operations Center (NOC) Engineer: - Monitor network performance and uptime. - Perform troubleshooting and resolve network outages. - Ensure 24/7 availability of services. Field Service Engineer : - Install and maintain mobile towers and related equipment. - Perform site inspections and ensure optimal equipment performance. 2. Datacenter Infrastructure Roles Datacenter Manager:(IT Manager) - Oversee datacenter operations and maintenance. - Ensure high availability and uptime of IT infrastructure. System Administrator - Manage servers, storage, and operating systems. - Perform regular system updates, backups,	OK

Clause No.	Requirement\\Departement	Evidence	Result
		and patches. Network Administrator - Configure and maintain network devices (routers, switches, firewalls). - Ensure secure and reliable connectivity in the datacenter. Information Security Specialist - Implement security policies. - Monitor for threats and vulnerabilities. - Ensure compliance with cybersecurity standards. Power and Cooling Technician - Maintain physical infrastructure within the datacenter. - Ensure proper cooling, power supply, and environmental controls. 3. Mobile Tower Installation Roles Tower Installation Engineer : - Oversee the installation of mobile towers - Ensure compliance with safety and technical standards. RF Engineer (Radio Frequency Engineer) - Design and optimize radio frequency networks. - Conduct RF site surveys and testing for tower installations. Site Acquisition Specialist - Identify and secure locations for mobile towers. - Negotiate with landowners and obtain necessary permits. 4. ICT Services and Technical Support Roles Network Engineer : - Design and deploy telecommunications networks. - Troubleshoot network connectivity issues. Telecom Engineer : - Maintain and troubleshoot telecom infrastructure (e.g., fiber optics, microwave links). 5. Amdinstartion Department Human Resource Manager details roles and responsibilities according to KSA laws : 1. Talent Acquisition and Recruitment Roles: Develop job descriptions for technical and	

Clause No.	Requirement\\Departement	Evidence	Result
		operational roles (e.g., engineers, technicians, IT specialists). Collaborate with department heads to identify staffing needs, especially for niche technical roles like RF Engineers or Datacenter Administrators. Conduct recruitment drives, interviews, and onboarding for technical and non-technical staff. Build partnerships with universities and technical institutes to attract skilled candidates. 2. Workforce Planning Roles: Plan workforce requirements for telecom projects, datacenter operations, and IT service delivery. Ensure the availability of skilled personnel for critical projects (e.g., mobile tower installations or datacenter upgrades). Manage employee allocation to different projects based on expertise and workload. 3. Training and Development Roles: Organize training programs to upskill employees in areas like: ICT services (networking, cloud, RF technology). Safety protocols for mobile tower installations. Cybersecurity and datacenter management. Facilitate certifications for employees in industry-relevant fields (e.g., Cisco, AWS, or ITIL certifications). Conduct workshops on soft skills, leadership, and time management. 4. Employee Performance Management Roles: Set KPIs (Key Performance Indicators) and performance goals for employees in technical and administrative roles. Conduct periodic performance reviews and appraisals. Identify high-performing employees for promotions or bonuses. Address underperformance through performance improvement plans (PIPs).	

Clause No.	Requirement\\Departement	Evidence	Result
		5. HR Policies and Compliance Roles: Develop HR policies that align with labor laws in Saudi Arabia (e.g., working hours, overtime, benefits). Ensure compliance with health and safety regulations, particularly for fieldwork like mobile tower installations. Handle employee grievances and disputes while ensuring fairness and adherence to company policies. Ensure compliance with Saudization (Nitaqat) requirements by hiring the mandated percentage of Saudi nationals. 6. Compensation and Benefits Management Roles: Design competitive salary packages to attract and retain skilled professionals. Manage employee benefits like health insurance, transportation allowances, and retirement plans. Oversee payroll processes and ensure timely salary disbursements. Provide incentives for employees working under challenging conditions (e.g., field engineers at remote tower sites). 7. Health, Safety, and Well-being Roles: Develop and enforce health and safety guidelines, particularly for employees working on mobile tower installations. Organize safety training for field engineers and technicians. Provide resources for employee well-being, such as counseling services or stress management workshops. Monitor compliance with workplace safety standards. 8. Employee Engagement Roles: Foster a positive work culture that promotes collaboration between technical and non-technical teams. Organize team-building activities and events to boost morale. Conduct regular employee satisfaction surveys and address feedback.	

Clause No.	Requirement\\Departement	Evidence	Result
		Recognize and reward employee contributions through awards or recognition programs. 9. HR Technology and Data Management Roles: Implement and maintain HR software for managing employee records, performance reviews, and payroll. Use analytics to monitor workforce trends (e.g., turnover rates, training needs). Ensure data privacy and security, especially for employee information stored digitally. 10. Strategic HR Planning Roles: Align HR strategies with the company's business goals, such as expanding ICT services or scaling datacenter operations. Develop succession plans to ensure leadership continuity in critical roles. Collaborate with senior management to forecast future talent needs, especially for emerging technologies like 5G or cloud services. 11. Conflict Resolution Roles: Act as a mediator in disputes between employees or teams. Handle conflicts related to project deadlines, resource allocation, or workplace behavior. Ensure fair and ethical resolution of issues. 12. Saudization (Nitaqat Program) Compliance Roles: Hire and train Saudi nationals to fulfill government-mandated quotas. Develop programs to integrate Saudi employees into technical roles. Ensure reporting to regulatory bodies regarding Saudization efforts. Key Competencies for an HR Manager in This Industry Technical Understanding: Knowledge of ICT services, telecom infrastructure, and datacenter operations. Regulatory Compliance: Awareness of labor laws, safety standards, and Saudization	

Clause No.	Requirement\\Departement	Evidence	Result
		requirements in KSA. People Management: Strong leadership, conflict resolution, and communication skills. Project Coordination: Ability to manage HR needs for large-scale projects like mobile tower installations. Analytical Skills: Use of HR analytics to drive decisions on recruitment, training, and performance management. -	
6.1	Actions to address risks and opportunities	Check Risk Managment Criteria from stage 1 which as follows : 3 matries High , Med, Low and each one 5x5 with compinations between severity and probability , High related to any service or security impact on BCM for the organization and med. related to any service or security impact to client assests or client services and Low related to any internal non impacted to client nor its services.	OK
6.1.2 ISO 27001	Information security risk assessment	check risk register and related Annexs with the following samples Risk Scenario: Laptops are used without antivirus software Impact: Malware infection or data theft Vulnerability: Lack of endpoint protection Threats: Malware, ransomware attacks Recommended Measure: Install and regularly update antivirus software on all laptops. Implement endpoint detection and response (EDR) solutions to monitor and block threats. Document: ANTI VIRUS CASPERSKY UPDATED LAST VERSION SERVER MANAGED, Dec. 2025	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Existing Control: Antivirus - McAfee - Ver.xxxxx Annex Ref.: A.8.23, A.5.7, A.8.7 Risk Scenario: Router uses default credentials Impact: Unauthorized access to router configuration Vulnerability: Default username and password Threats: Brute-force attacks, unauthorized access Recommended Measure: Change default credentials, enforce strong passwords, and disable unused administrator accounts on routers. Document: PASSWORD POLICY within acceptable usage policy IT-PO-03 Existing Control: Admin Password / changed credentials Annex Ref.: A.8.23, A.5.9 Risk Scenario: Google Forms data shared publicly due to incorrect sharing settings Impact: Data leakage or unauthorized access Vulnerability: Lack of data classification policy Threats: Human error, insider threats Recommended Measure: Train employees to configure sharing settings properly, implement access reviews, and enforce data classification policies. Document: Data classification over ERP TRIO SYSTEM, awareness meetings and announcements, Access control policy IT-PR-07 Existing Control: Use of access policy Annex Ref.: A.8.33, A.5.16 Risk Scenario: Laptops not updated with security patches Impact: Exploitation of known vulnerabilities Vulnerability: Lack of patch management Threats: Exploitation of unpatched vulnerabilities Recommended Measure: Implement a	

Clause No.	Requirement\\Departement	Evidence	Result
		patch management system to ensure all laptops are updated with the latest security patches and updates. Document: WINDOWS update enforced through group policy, antivirus alert with updates through the system Existing Control: Implemented Annex Ref.: A.5.23, A.5.26 Risk Scenario: No multi-factor authentication (MFA) for Google Forms Impact: Unauthorized access to Google Forms Vulnerability: Single-factor authentication Threats: Credential theft, brute-force attacks Recommended Measure: Enforce MFA for all Google accounts to add a second layer of security and reduce reliance on passwords. Document: All Microsoft accounts are MFA Existing Control: Implemented on Microsoft Annex Ref.: A.5.7, A.5.9 Risk Scenario: Router firmware is outdated Impact: Exploitation of known firmware vulnerabilities Vulnerability: Lack of firmware updates Threats: Exploitation of unpatched vulnerabilities Recommended Measure: Regularly update router firmware to the latest version and subscribe to vendor security advisories to stay informed about critical updates. Document: Firewall update as per Fortinet USA patches Existing Control: Annex Ref.: A.5.23, A.5.26 Risk Scenario: Employees use personal laptops to access corporate Google Forms Impact: Data leakage or malware infection Vulnerability: Lack of device management policies Threats: Compromised personal devices Recommended Measure: Enforce device management policies, restrict access to trusted devices only, and implement	

Clause No.	Requirement\\Departement	Evidence	Result
		endpoint security solutions. Document: Endpoint security by Kaspersky, IT-PO-04 mobile computing and communication policy, network segregation, domain account required even for personal laptops Existing Control: Personal laptop not allowed Annex Ref.: A.8.23, A.5.8 Risk Scenario: Weak passwords used for Google accounts Impact: Unauthorized access to sensitive data Vulnerability: Lack of password policy Threats: Password guessing, brute-force attacks Recommended Measure: Enforce strong password policies, require password complexity, and implement password expiration policies. Document: PASSWORD POLICY within acceptable usage policy IT-PO-03 Existing Control: Implemented Annex Ref.: A.5.9, A.5.12 Risk Scenario: No centralized monitoring for Google Forms access Impact: Unauthorized access goes unnoticed Vulnerability: Lack of monitoring and logging Threats: Insider threats, unauthorized access Recommended Measure: Enable centralized logging and monitoring for Google Forms, and configure alerts for unusual access patterns or activities. Document: Log history over TRI system monitored centrally Existing Control: Implemented Annex Ref.: A.5.28, A.5.29 Risk Scenario: Laptops lack encryption for local storage of sensitive data Impact: Data theft in case of laptop theft/loss	

Clause No.	Requirement\\Departement	Evidence	Result
		Vulnerability: No encryption for local files Threats: Physical theft or device loss Recommended Measure: Enable full-disk encryption on laptops and ensure sensitive files are encrypted by default. Document: All USB ports are closed and data transfer through the system only Existing Control: Awareness & policy for sensitive data storage Annex Ref.: A.5.18, A.8.33 Risk Scenario: Employees use public Wi-Fi without VPN Impact: Data interception during transmission Vulnerability: No encryption on public networks Threats: Eavesdropping, session hijacking Recommended Measure: Enforce VPN usage for all employees when working on public Wi-Fi, and educate employees on risks of insecure networks. Document: Acceptable usage policy IT-PO-03 Existing Control: Implemented Annex Ref.: A.5.13, A.5.14 Risk Scenario: No backup for critical Google Forms data Impact: Data loss from accidental deletion or attacks Vulnerability: Lack of data backup policy Threats: Accidental deletion, ransomware Recommended Measure: Implement a regular backup policy for Google Forms data, ensure backups are encrypted, and store them in a secure location. Document: Operations security policy IT-PO-15 Pt. 6 Existing Control: Implemented Annex Ref.: A.5.30, A.8.29 Risk Scenario: Laptops lack physical security measures Impact: Theft or unauthorized access to devices Vulnerability: No physical security controls Threats: Theft, unauthorized physical	

Clause No.	Requirement\\Departement	Evidence	Result
		access Recommended Measure: Implement physical security measures such as cable locks, secure storage for laptops, and training employees to secure their devices in public spaces. Document: Physical security policy IT-PO-16 Existing Control: Awareness for keeping laptops secure from theft Annex Ref.: A.7.4, A.8.23 Risk Scenario: No periodic review of Google Forms access permissions Impact: Unauthorized users retain access to sensitive data Vulnerability: Stale or outdated permissions Threats: Insider threats, human error Recommended Measure: Conduct periodic reviews of access to Google Forms, remove access for inactive users, and enforce least privilege access principles. Document: Access control procedure IT-PR-07 Existing Control: Implemented Annex Ref.: A.5.16, A.5.18 Risk Scenario: Shared passwords among employees for accessing Google Forms Impact: Unauthorized access to sensitive data Vulnerability: Lack of unique authentication Threats: Insider threats, credential theft Recommended Measure: Prohibit password sharing, enforce unique accounts for all employees, and enable multi-factor authentication (MFA) to improve security. Document: Acceptable usage policy IT-PO-03, Announcements Existing Control: Implemented Annex Ref.: A.5.9, A.5.12 Risk Scenario: No logging of failed login attempts for Google accounts Impact: Brute-force attacks go undetected Vulnerability: Lack of monitoring and alerting	

Clause No.	Requirement\\Departement	Evidence	Result
		Threats: Unauthorized access attempts Recommended Measure: Enable logging of failed login attempts in Google Workspace, configure alerts for suspicious activity, and review logs regularly. Document: Logging over ERP TRIO SYSTEM monitoring, Microsoft accounts have limited logging trials Existing Control: Implemented Annex Ref.: A.5.28, A.5.29 Risk Scenario: Employees save sensitive data locally on laptops Impact: Data theft or unauthorized access Vulnerability: No centralized data storage policy Threats: Physical theft, malware Recommended Measure: Implement a centralized data storage policy, restrict local data storage, and enable encryption for any locally stored sensitive files. Document: Operations security policy IT-PO-15 Pt. 6 Existing Control: Awareness & policy for sensitive data storage Annex Ref.: A.5.18, A.8.33 Risk Scenario: No restriction on file sharing for Google Forms Impact: Data leakage or unauthorized sharing Vulnerability: Lack of file sharing policies Threats: Insider threats, accidental sharing Recommended Measure: Restrict file sharing settings for Google Forms, implement role-based access controls (RBAC), and monitor shared files for unusual activity. Document: No shared folder, OneDrive sharing restrictions (view-only files) Existing Control: Implemented Annex Ref.: A.5.16, A.8.30 Risk Scenario: Lack of device tracking for laptops Impact: Inability to recover lost or stolen devices	

Clause No.	Requirement\\Departement	Evidence	Result
		Vulnerability: No asset management system Threats: Theft, loss of devices Recommended Measure: Implement a device inventory and tracking system, use asset tagging, and deploy remote wipe capabilities to secure lost or stolen devices. Document: Asset inventory over ERP TRIO system, IT-PR-03 Asset classification, IT-PO-06 Asset management policy Existing Control: Implemented Annex Ref.: A.8.23, A.5.27 Risk Scenario: Employees do not log out from shared Google Forms access Impact: Unauthorized access after session ends Vulnerability: No session management policy Threats: Insider threats, accidental misuse Recommended Measure: Enforce session timeouts and automatic logouts for inactivity, and train employees to manually log out of Google Forms sessions on shared devices. Document: Announcements Existing Control: Awareness Annex Ref.: A.5.17, A.5.28 Risk Scenario: Employees click on phishing links targeting Google Forms Impact: Credential theft or data compromise Vulnerability: Lack of phishing awareness training Threats: Phishing attacks, social engineering Recommended Measure: Conduct regular phishing awareness training, simulate phishing tests, and implement email filtering solutions to block phishing emails. Document: Spam expert for mail classification, Announcements, IT-PO-03 Acceptable use policy Existing Control: Implemented Annex Ref.: A.7.2, A.5.7 Risk Scenario: Laptops are shared among multiple users	

Clause No.	Requirement\\Departement	Evidence	Result
		Impact: Unauthorized access to sensitive data Vulnerability: Lack of user segregation Threats: Insider threats, accidental access Recommended Measure: No multiple users allowed on laptops. Document: Employee custody, IT-PO-03 Acceptable use policy Existing Control: Implemented Annex Ref.: A.5.9, A.7.4 Risk Scenario: No monitoring of Google Forms data access patterns Impact: Suspicious activity goes undetected Vulnerability: Lack of anomaly detection Threats: Insider threats, unauthorized access Recommended Measure: Deploy monitoring tools to detect unusual access patterns, configure alerts for anomalies, and review Google Workspace activity logs regularly. Document: Log monitor for all transactions and unusual activity Existing Control: Implemented Annex Ref.: A.5.28, A.5.29 Risk Scenario: Employees store sensitive passwords in browser autofill Impact: Credential theft Vulnerability: No password management policy Threats: Malware, unauthorized access Recommended Measure: Prohibit storing passwords in browser autofill, enforce the use of password managers, and train employees on secure password storage practices. Document: PASSWORD POLICY within acceptable usage policy IT-PO-03 Existing Control: Awareness Annex Ref.: A.5.12, A.8.33 Risk Scenario: Google Forms links are shared in public forums Impact: Unauthorized access to forms and data Vulnerability: Lack of access restrictions Threats: Data leakage, insider threats	

Clause No.	Requirement\\Departement	Evidence	Result
		Recommended Measure: Restrict sharing settings to authorized users only, and monitor for publicly accessible links using tools to detect exposed links. Document: Sharing policies over OneDrive and ERP TRIO Existing Control: Implemented by separate folders Annex Ref.: A.5.16, A.8.30 Risk Scenario: No restrictions on installation of software on laptops Impact: Installation of untrusted or malicious software Vulnerability: Lack of application control policies Threats: Malware, ransomware Recommended Measure: Implement application control policies, restrict installation of unauthorized software, and use endpoint security solutions to monitor and block malicious applications. Document: All laptops on domain, and users are local accounts with no admin privileges Existing Control: Admin control Annex Ref.: A.5.26, A.5.7 Risk Scenario: Google Forms data accessed without encryption Impact: Data interception during transmission Vulnerability: Lack of encryption for data in transit Threats: Man-in-the-middle (MITM) attacks Recommended Measure: Enforce HTTPS for all Google Forms access, implement VPNs for insecure networks, and restrict access to trusted and encrypted connections only. Document: Over system only HTTPS is authorized Existing Control: Implemented Annex Ref.: A.5.14, A.8.23 Risk Scenario: No incident response plan for Google Forms breaches	

Clause No.	Requirement\\Departement	Evidence	Result
		Impact: Delayed response to breaches or attacks Vulnerability: Lack of incident management process Threats: Data breaches, reputational damage Recommended Measure: Develop an incident response plan for Google Forms, conduct regular incident response drills, and ensure employees understand reporting procedures. Document: IT-PO-05 incident management policy Existing Control: Implemented Annex Ref.: A.5.33, A.5.34 Risk Scenario: Employees use personal cloud storage for Google Forms data Impact: Data leakage or loss Vulnerability: Lack of data storage policies Threats: Insider threats, unauthorized access Recommended Measure: Prohibit the use of personal cloud storage for corporate data, enforce storage in approved locations, and monitor for unauthorized data transfers. Document: Only corporate OneDrive account is allowed Existing Control: Awareness & policy for sensitive data storage Annex Ref.: A.5.18, A.8.33 Risk Scenario: No protection against brute-force attacks targeting routers Impact: Unauthorized access to network infrastructure Vulnerability: Weak or reused router credentials Threats: Brute-force attacks, credential attacks Recommended Measure: Implement account lockout mechanisms, enforce strong router passwords, and monitor for repeated failed login attempts on network infrastructure devices. Document: Domain control policy Existing Control: Implemented	

Clause No.	Requirement\\Departement	Evidence	Result
		Annex Ref.: A.5.9, A.5.29 Risk Scenario: Employees use weak passwords for router admin accounts Impact: Unauthorized access to router configuration Vulnerability: Weak password policies Threats: Brute-force attacks, credential theft Recommended Measure: Enforce strong password policies for router admin accounts, require password complexity, and rotate passwords periodically. Document: IT-PO-03 acceptable use policy Existing Control: Implemented Annex Ref.: A.5.9, A.5.12 Risk Scenario: No multi-factor authentication (MFA) for router admin access Impact: Compromise of router admin accounts Vulnerability: Single-factor authentication Threats: Credential theft, unauthorized access Recommended Measure: Implement MFA for router admin accounts to add an additional layer of security against credential theft. Document: IT-PO-03 acceptable use policy Existing Control: Implemented Annex Ref.: A.5.9, A.5.7 Risk Scenario: Google Forms data is stored without encryption in the cloud Impact: Data exposure in case of a breach Vulnerability: Lack of encryption for data at rest Threats: Data breaches, insider threats Recommended Measure: Enable encryption for data at rest in Google Workspace, and review encryption settings to ensure compliance with security policies. Document: Password-protected backups; all backups are encrypted Existing Control: Implemented Annex Ref.: A.8.33, A.5.18	

Clause No.	Requirement\\Departement	Evidence	Result
		Risk Scenario: No logging of router configuration changes Impact: Unauthorized changes go undetected Vulnerability: Lack of change monitoring Threats: Insider threats, misconfigurations Recommended Measure: Enable logging for router configuration changes, monitor logs regularly, and configure alerts for unusual or unauthorized changes. Document: Router is managed by ISP Existing Control: Implemented Annex Ref.: A.5.28, A.5.29 Risk Scenario: Employees use personal email accounts to access Google Forms Impact: Data leakage from unmonitored accounts Vulnerability: Lack of access control enforcement Threats: Insider threats, unauthorized access Recommended Measure: Restrict access to Google Forms to corporate email accounts only, and monitor access to ensure compliance with organizational policies. Document: Sharing policies over OneDrive and ERP TRIO Existing Control: Implemented Annex Ref.: A.5.16, A.8.30 Risk Scenario: No restrictions on copying and pasting data from Google Forms Impact: Data leakage through unprotected endpoints Vulnerability: Lack of endpoint protection Threats: Insider threats, accidental data sharing Recommended Measure: Implement endpoint detection and response (EDR) solutions, restrict copy-paste functionality for sensitive data, and monitor endpoint activity. Document: EDR over Kaspersky Existing Control: Implemented Annex Ref.: A.8.30, A.5.7	

Clause No.	Requirement\\Departement	Evidence	Result
		Risk Scenario: Employees do not report suspicious activity on Google Forms Impact: Delayed response to potential security breaches Vulnerability: Lack of security awareness training Threats: Insider threats, phishing attacks Recommended Measure: Provide regular security awareness training, establish reporting mechanisms for suspicious activity, and encourage employees to report potential threats promptly. Document: Announcements and trainings Existing Control: Implemented Annex Ref.: A.7.2, A.5.34 Risk Scenario: No control over external sharing of Google Forms Impact: Data leakage to unauthorized parties Vulnerability: Lack of external sharing policies Threats: Insider threats, accidental sharing Recommended Measure: Restrict external sharing of Google Forms, implement approval workflows for external sharing requests, and monitor shared links for unusual activity. Document: Sharing policies over OneDrive and ERP TRIO Existing Control: Implemented Annex Ref.: A.5.16, A.8.30 Risk Scenario: Laptops are not protected with screen lock policies Impact: Unauthorized access to devices left unattended Vulnerability: Lack of session control Threats: Insider threats, accidental misuse Recommended Measure: Enforce screen lock policies with short inactivity timeouts, and train employees to lock their screens manually when stepping away from their devices. Document: IT-PO-03 acceptable use policy Existing Control: Implemented Annex Ref.: A.5.17, A.8.23	

Clause No.	Requirement\\Departement	Evidence	Result
		Risk Scenario: No firewall configured for routers Impact: Network is exposed to unauthorized traffic Vulnerability: Lack of network segmentation Threats: Malware, unauthorized access Recommended Measure: Configure firewalls on routers to restrict unauthorized traffic, enable intrusion detection systems (IDS), and segment networks for added protection. Document: We use our own firewall Existing Control: Implemented Annex Ref.: A.5.13, A.8.23 Risk Scenario: Employees use unauthorized USB devices Impact: Malware infection or data exfiltration Vulnerability: Lack of endpoint control policies Threats: Malware, insider threats Recommended Measure: Restrict the use of unauthorized USB devices, enable USB port control policies, and scan all connected devices for malware. Document: All USB ports are closed, and data transfer is through the system only Existing Control: Implemented Annex Ref.: A.5.7, A.8.23 Risk Scenario: Outdated firmware on routers Impact: Vulnerabilities in network infrastructure Vulnerability: Lack of patch management Threats: Exploits, malware Recommended Measure: Implement a patch management process to regularly update router firmware and monitor for vendor-released patches. Document: All routers are connected to the firewall, and patches are updated regularly Existing Control: Implemented Annex Ref.: A.5.26, A.5.29 Risk Scenario: Employees use unapproved third-party apps with Google Forms	

Clause No.	Requirement\\Departement	Evidence	Result
		Impact: Data leakage or compromised integrations Vulnerability: Lack of application control policies Threats: Exploits, data breaches Recommended Measure: Restrict the use of unapproved applications, implement app whitelisting policies, and review third-party app integrations for security risks. Document: All employees are local users only Existing Control: Admin control Annex Ref.: A.5.19, A.8.33 Risk Scenario: No monitoring for failed router login attempts Impact: Brute-force attacks go undetected Vulnerability: Lack of security monitoring Threats: Unauthorized access attempts Recommended Measure: Enable logging for failed router login attempts, configure alerts for suspicious activity, and review logs regularly. Document: All login cases are sent to the IT team, awareness and training are conducted regularly Existing Control: Implemented Annex Ref.: A.5.28, A.5.29 Risk Scenario: Employees lack training on secure Google Forms sharing Impact: Data leakage from improper sharing Vulnerability: Lack of security awareness training Threats: Insider threats, accidental sharing Recommended Measure: Provide employees with regular training on securely sharing Google Forms, and enforce policies to restrict unnecessary data sharing. Document: Domain control policy Existing Control: Implemented Annex Ref.: A.7.2, A.5.16 Risk Scenario: No security review of Google Forms templates Impact: Templates may include vulnerable configurations	

Clause No.	Requirement\\Departement	Evidence	Result
		Vulnerability: Lack of security reviews Threats: Insider threats, misconfigurations Recommended Measure: Conduct regular security reviews of Google Forms templates, and standardize secure templates for sensitive data collection. Document: Domain control policy Existing Control: Implemented Annex Ref.: A.5.26, A.8.30 Risk Scenario: No centralized inventory of active Google Forms Impact: Lack of visibility into sensitive data Vulnerability: No inventory management Threats: Insider threats, data leakage Recommended Measure: Create a centralized inventory of Google Forms, monitor for unauthorized or inactive forms, and classify forms based on sensitivity. Document: All logs are monitored and registered Existing Control: Implemented Annex Ref.: A.5.27, A.8.23 Risk Scenario: Shared credentials for router admin accounts Impact: Unauthorized access to router configuration Vulnerability: Lack of individual accountability Threats: Insider threats, credential theft Recommended Measure: Prohibit shared credentials for router admin accounts, enforce unique accounts for each admin, and enable logging to track account activity. Document: IT-PR-02 information management procedure Existing Control: Implemented Annex Ref.: A.5.9, A.5.28 Risk Scenario: Employees use personal devices to access Google Forms Impact: Data leakage through unprotected endpoints Vulnerability: Lack of BYOD (Bring Your Own Device) policy Threats: Malware, unauthorized data	

Clause No.	Requirement\\Departement	Evidence	Result
		transfers Recommended Measure: Implement a BYOD policy requiring security controls on personal devices, such as encryption and endpoint security solutions. Document: IT-PO-04 mobile computing policy, IT-PO-03 acceptable use policy Existing Control: Implemented Annex Ref.: A.8.23, A.5.7 Risk Scenario: No security testing of Google Forms integrations Impact: Vulnerabilities in third-party integrations Vulnerability: Lack of security testing Threats: Exploits, malware Recommended Measure: Conduct regular security testing of Google Forms integrations, assess third-party apps for vulnerabilities, and disable unused integrations. Document: IT-PR-05 vulnerability procedure Existing Control: No add-on allowed Annex Ref.: A.5.26, A.5.19 Risk Scenario: No backup strategy for Google Forms data Impact: Permanent loss of critical data Vulnerability: Lack of data backup policy Threats: Accidental deletion, ransomware attacks Recommended Measure: Implement a backup strategy for Google Forms data, ensure backups are performed regularly, and test recovery procedures periodically. Document: Over ERP TRIO and VEEM backup server, IT-PR-01 CCTV backup Existing Control: Implemented Annex Ref.: A.5.30, A.8.28 Risk Scenario: Employees reuse passwords across different accounts Impact: Credential theft and account compromise Vulnerability: Weak password management practices Threats: Phishing attacks, brute-force	

Clause No.	Requirement\\Departement	Evidence	Result
		attacks Recommended Measure: Enforce a password policy, require unique passwords for accounts, and implement password management tools to help employees avoid reuse. Document: IT-PO-03 acceptable use policy Existing Control: Implemented Annex Ref.: A.5.9, A.5.12 Risk Scenario: No restrictions on access to Google Forms from public devices Impact: Unauthorized access to sensitive data Vulnerability: Lack of device access controls Threats: Credential theft, data breaches Recommended Measure: Restrict access to Google Forms from unmanaged or public devices, enforce device trust policies, and require multi-factor authentication (MFA). Document: IT-PO-03 acceptable use policy, IT-PO-04 MOBILE Existing Control: Implemented Annex Ref.: A.5.16, A.5.9 Risk Scenario: Employees share Google Forms passwords via email Impact: Credential theft Vulnerability: Lack of secure credential sharing Threats: Phishing attacks, insider threats Recommended Measure: Prohibit sharing passwords via email, train employees on secure credential sharing practices, and use password managers with secure sharing features. Document: IT-PO-03 acceptable use policy Existing Control: Awareness Annex Ref.: A.5.12, A.7.2	
6.1.3 ISO 27001	Information security risk treatment	All risk treatment from Clause 6.1.2 have been implmented with approvals from Eng. Shadi Al-Tamimi IT group Manager as risk owner during Teams meeting	OK

Clause No.	Requirement\\Departement	Evidence	Result
6.2	Service & Information security management objectives and planning to achieve them	6.2.1 Establish objectives Check Objective for upgrading Trio-Application in House by 2026 to cover new required services. by Q3 in 2026 Also check physical security objective which required to install access control gate connected to attendance and identity managment , the gate planed to be installed and run by Q2 2026 6.2.2 Plan to achieve objectives Action plans with resources are in place for both checked objectives last Managment review assign budget and resources for these both objectives.	OK
6.3	Plan the service management system and IS changes	Serivce Managment plan established and implmeneted The service management plan shall include : a) list of services; b) known limitations which reflected in issue register c) obligations such as relevant policies, standards, legal, regulatory and contractual requirements, are addressed in table for interetsed parties and their requirements (See 4.2 in this report) d) All job descriptions are doucmented and organization chart are included in SMP with refernce to all authorities and responsibilities for the SMS ,ISMS and the services; which managed by HR department e) All determined human, technical, information and financial resources necessary to operate the SMS and the services are assigend in Asset register for Datacenter assests and also for human assets in HR department , other finaicial resources are defined in Trio- Application f) approach to be taken for working with other parties involved in the service lifecycle; g) Data center technology used to support the SMS are defined ;Host Processor: Intel Xeon Processor D- Host Memory: 16 GB DDR4	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Host Storage: 4 TB RAID 5 Host OS: VMware Host Application: APPSHARE SERVER VM Name: ICC Hostname / Server Name: 172.16.1.1 Virtual Machines: 3 CPU: 4 RAM: 8 GB Storage: 1 TB Host Storage Remaining: 3 TB Host Processor: Intel Xeon Processor D- Host Memory: 32 GB DDR4 Host Storage: 6 TB RAID 5 Host OS: VMware Host Application: Backup/Archiving (Acting Backup Host) VM Name: BACKUP Hostname / Server Name: 172.16.1.2 Virtual Machines: 4 CPU: 8 RAM: 16 GB Storage: 2 TB Host Storage Remaining: 4 TB Host Processor: Intel Xeon Processor D- Host Memory: 64 GB DDR4 Host Storage: 4 TB RAID 1 Host OS: Microsoft Hyper-V Host Application: TrendAV VM Name: TRENDAV Hostname / Server Name: 172.16.2.1 Virtual Machines: 2 CPU: 4 RAM: 32 GB Storage: 1 TB Host Storage Remaining: 3 TB Host Processor: Intel Xeon Processor D- Host Memory: 16 GB DDR4 Host Storage: 8 TB RAID 6 Host OS: VMware Host Application: SQL (Primary SQL Server) VM Name: PRIMARYSQL Hostname / Server Name: 172.16.2.2 Virtual Machines: 5	

Clause No.	Requirement\\Departement	Evidence	Result
		CPU: 4 RAM: 16 GB Storage: 4 TB Host Storage Remaining: 4 TB Host Processor: Intel Xeon Processor D- Host Memory: 32 GB DDR4 Host Storage: 8 TB RAID 6 Host OS: VMware Host Application: Veeam Server VM Name: VEEAMSERVER Hostname / Server Name: 172.16.2.3 Virtual Machines: 2 CPU: 8 RAM: 32 GB Storage: 4 TB Host Storage Remaining: 4 TB h) Comperhnisve datshboard are used in trio-application for all activivties for monitoring the effectiveness of the SMS and the services with reporting.	
7.1	Resources	all required resources have been determined and provided , the approved resources required managed by IT group manager with the board for Bazy	OK

Clause No.	Requirement\\Departement	Evidence	Result
7.2	Competence /HR	HR recurrutment process for workflow for jop post #17077 this iniiated by HR manager ID # 2272 , then PM approval ID # 2488 , if Ok then OM checks #2490 , then Business Unit manager #2489 approval for competency and experiance check approval then finaice officer #2522 for salary agreements. NDA shall be signed with contract. From Trio-application (HR dashboard) select employee #4436 name :Nasser Mansour El shile HR manager , he graduated from Yanboa Univeristy bachalor of sience in managent of information systems and then post graduate study for MIS specialization certifcate in ERP-Systems from same universty all employee documents are uploaded into the system (certifcates - ID - CV - contract (A6.2 Terms and conditions of employment) - NDA (A6.6 Confidentiality or non-disclosure agreements) - Signed job description including his resposnibility and authority (A5.2 Information security roles and responsibilities) and check for his duty with other empoyees the previllages in software ensure segregation of employee duty (A5.3 Segregation of duties) to eliminate Conflicting duties and conflicting areas of responsibility. Evaluation for employee criteria are in trio-application (10 criterias) like production quantity ,learning , performance quality and attendance .	OK
7.3	Awareness	check emails send to all emplyees related to awarness about phising attacks.	OK
7.4	Communication	check internal communication with employee related to awarness for phising attacks by email and external communicating with external providers through VPNs or Authority portal applications	OK

Clause No.	Requirement\\Departement	Evidence	Result
7.5	Documented information	document control procedure (See stage 1 audit report) with available master list of documents MLD this determined with risks related to (A8.13) backup policy , (A8.24) encryptions and (A5.33) protection of records ,(A5.32) Intellectual property rights ,(A7.10)Storage media,(A8.10)Information deletion and checked some related risk 1. A.5.12: Classification of Information Risk Scenario: Misclassification of documents leads to unauthorized access or improper handling. Threats: Insider threats, accidental sharing, unauthorized access. Impact on CIA: C: Misclassified documents are accessed by unauthorized users. I: Poor classification can lead to errors in handling critical data. A: Difficulty in locating essential documents quickly. Control: Establish and enforce an information classification policy to categorize and protect documents based on their sensitivity. 2. A.5.13: Labeling of Information Risk Scenario: Lack of labeling results in sensitive documents being mishandled. Threats: Human error, compliance violations. Impact on CIA: C: Unlabeled sensitive documents may be accessed by unauthorized parties. I: Lack of labeling may cause data corruption during handling. A: Retrieval of documents may become inefficient. Control: Implement mandatory labeling for all sensitive documents, indicating their classification and handling instructions. 3. A.8.9: Data Leakage Prevention Risk Scenario: Sensitive documents are leaked through unauthorized sharing or unprotected endpoints. Threats: Insider threats, accidental	OK

Clause No.	Requirement\\Departement	Evidence	Result
		disclosure. Impact on CIA: C: Unauthorized individuals may access confidential data. I: Leaked data could be altered maliciously. A: Loss of critical data affects operational availability. Control: Implement data leakage prevention (DLP) solutions to monitor and prevent unauthorized sharing of sensitive information. 4. A.8.10: Monitoring Activities Risk Scenario: Unauthorized access to sensitive documents goes undetected due to lack of monitoring. Threats: Insider threats, data breaches. Impact on CIA: C: Sensitive information could be accessed by malicious actors. I: Alterations to documents may go unnoticed. A: Lack of monitoring may delay discovering unavailability issues. Control: Enable monitoring of document access and modification activities, and configure alerts for suspicious behavior. 5. A.5.7: Inventory of Information and Other Associated Assets Risk Scenario: Untracked documents lead to loss or unauthorized access. Threats: Poor asset management, theft, unauthorized access. Impact on CIA: C: Untracked sensitive documents may be accessed by unauthorized users. I: Unmanaged documents could be corrupted. A: Failure to locate critical documents in a timely manner. Control: Maintain an inventory of all critical documents and associated storage locations. 6. A.8.12: Sensitive Data Transfers Risk Scenario: Sensitive documents are transmitted without encryption, exposing them to interception. Threats: Man-in-the-middle (MITM) attacks,	

Clause No.	Requirement\\Departement	Evidence	Result
		data interception. Impact on CIA: C: Sensitive data may be exposed during transmission. I: Intercepted data could be altered. A: Interference with the transfer process could delay access to critical documents. Control: Enforce encryption for sensitive data during transfers and use secure protocols (e.g., HTTPS, SFTP). 7. A.5.16: Access Control Policy Risk Scenario: Unauthorized access to documents due to poor access control policies. Threats: Insider threats, external attackers. Impact on CIA: C: Unauthorized individuals may access confidential documents. I: Documents may be altered or deleted maliciously. A: Legitimate users may lose access to the documents. Control: Implement an access control policy to enforce least privilege principles and role-based access control (RBAC). 8. A.5.21: Backup Risk Scenario: Documents are lost due to insufficient or failed backups. Threats: System failures, ransomware attacks, accidental deletion. Impact on CIA: C: Backups may expose sensitive data if not encrypted. I: Corrupted backups could restore incorrect data. A: Delays in document recovery may affect operational availability. Control: Perform regular backups of critical documents, ensure encryption of the backups, and test recovery processes. 9. A.5.30: Information Security Incident Reporting Risk Scenario: Employees fail to report document-related incidents, delaying response. Threats: Insider threats, delayed response to breaches.	

Clause No.	Requirement\\Departement	Evidence	Result
		Impact on CIA: C: Sensitive documents remain exposed for longer periods. I: Alterations to documents might not be rectified in time. A: Lack of timely reporting may result in data loss or downtime. Control: Establish a clear incident reporting procedure for document-related security incidents. 10. A.7.4: Physical Security Monitoring Risk Scenario: Unauthorized individuals physically access documents stored on-site. Threats: Theft, physical tampering. Impact on CIA: C: Physical access to sensitive documents may compromise confidentiality. I: Tampered documents may lose their integrity. A: Theft or destruction of physical documents impacts availability. Control: Monitor physical access to document storage areas and implement controls such as surveillance cameras and access logs. Unauthorized Access to Documents: Threats: Insider threats, weak access controls. Impact on CIA: C: Leaked sensitive information. I: Unauthorized changes to critical documents. A: Legitimate users may lose access to required information. Loss of Critical Documents: Threats: Hardware failure, accidental deletion. Impact on CIA: C: Confidential data could be exposed if hardware is not securely disposed of. I: Loss of critical documents affects operational data integrity. A: Downtime due to lost documents impacts availability. Data Leakage during Transmission:	

Clause No.	Requirement\\Departement	Evidence	Result
		Threats: MITM attacks, lack of encryption. Impact on CIA: C: Sensitive data is exposed during transmission. I: Data altered during transmission could lead to errors. A: Disrupted transfers delay document availability.	
7.5.4	Service management system documented information	List of documented information have been reviewed within master list of document	OK
7.6	Knowledge	Bazy use risk managment as a tool for Knowledge management through the whole group and Assign QA manager to be responsible for it.	OK
8.1	Operational planning and control	All controls determined in 6.1 have been implemented , check physical security with facility manager , the track selected start from outside the building (A7.1) through the main enterance(A7.2) and upstrairs till IT room then datacenter room. check dome 360 Camera (A7.4) outdoor then inside entry the main H.Q Bazy building with Security Guard (A7.2) record visitor data(A7.4) , then upstairs to floor no. 1 which locate Datacenter , with IP camera (A7.4) which foucased on IT door with access control card (A7.3), and then interior IP camera inside IT room focuased on the IT and datacenter doors ,which use access control(A7.3) also for entering the datacenter room check datalog for access controls and IP cameras (A8.15) Logging. Privileged access rights(A8.2) assigned for IT manager and few dedicated IT team for entrance room , cameras are sycnhronized through server (A8.17) Clock synchronization	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.2.1 ISO 20000-1	Service portfolio \ Service delivery	Service delivery manager, division called (BAZY track) specialized in vehicle tracking and IOT, reviewed contracts between company and customers focusing on NDA and business continuity, customer credentials and critical information are governed contractually and segregation of responsibilities Clearance of employees process reviewed through ERP system (approvals, responsibilities, security)	OK
8.2.2 ISO 20000-1	Plan the services	check service requirements emails for updating Trio-Application for finaicial department and CRM. , the internal client high level requirements tracked to detailed requirements in SLAs .	OK
8.2.3 ISO 20000-1	Control of parties involved in the service lifecycle	2. procurement dept. Procedure reviewed with evidences from the procurement cycle through ERP SYSTEM(AWTAD company as a subcontractor sample) NDA is stated in the contract, knowledge transfer, and commitment to all regulations and legislations All service providers to the IT related issues are contracted as per KSA regulations (ORACLE contract for cloud storage as a sample) Vendors evaluations periodically each 6 month, with approved vendor list through ERP system Objectives of sustainable procurement to be applied by Q2 2026 Legal compliance reviewed through the matrix reviewed quarterly Supply chain reviewed	OK
8.2.4 ISO 20000-1	Service catalogue management	check Service catalogue including cloud and requirements.	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.2.5 ISO 20000-1	Asset management	Data Center Assests are defined : Host Processor: Intel Xeon Processor D- Host Memory: 16 GB DDR4 Host Storage: 4 TB RAID 5 Host OS: VMware Host Application: APPSHARE SERVER VM Name: ICC Hostname / Server Name: 172.16.1.1 Virtual Machines: 3 CPU: 4 RAM: 8 GB Storage: 1 TB Host Storage Remaining: 3 TB Host Processor: Intel Xeon Processor D- Host Memory: 32 GB DDR4 Host Storage: 6 TB RAID 5 Host OS: VMware Host Application: Backup/Archiving (Acting Backup Host) VM Name: BACKUP Hostname / Server Name: 172.16.1.2 Virtual Machines: 4 CPU: 8 RAM: 16 GB Storage: 2 TB Host Storage Remaining: 4 TB Host Processor: Intel Xeon Processor D- Host Memory: 64 GB DDR4 Host Storage: 4 TB RAID 1 Host OS: Microsoft Hyper-V Host Application: TrendAV VM Name: TRENDAV Hostname / Server Name: 172.16.2.1 Virtual Machines: 2 CPU: 4 RAM: 32 GB Storage: 1 TB Host Storage Remaining: 3 TB Host Processor: Intel Xeon Processor D- Host Memory: 16 GB DDR4 Host Storage: 8 TB RAID 6 Host OS: VMware Host Application: SQL (Primary SQL Server)	OK

Clause No.	Requirement\\Departement	Evidence	Result
		VM Name: PRIMARYSQL Hostname / Server Name: 172.16.2.2 Virtual Machines: 5 CPU: 4 RAM: 16 GB Storage: 4 TB Host Storage Remaining: 4 TB Host Processor: Intel Xeon Processor D- Host Memory: 32 GB DDR4 Host Storage: 8 TB RAID 6 Host OS: VMware Host Application: Veeam Server VM Name: VEEAMSERVER Hostname / Server Name: 172.16.2.3 Virtual Machines: 2 CPU: 8 RAM: 32 GB Storage: 4 TB Host Storage Remaining: 4 TB and complete cycle for Asset deivery till return of assets are controlled by IT manager and HR	
8.2.6 ISO 20000-1	Configuration management	check configrations for core switch for port security and practically test during the audit Cisco script for HR VLAN devices.	OK
8.3.1 ISO 20000-1	Relationship and agreement	check agreements documneted agreement between supplier and	OK
8.3.2 ISO 20000-1	Business relationship management	Assigned Business relation for each client check STC and Nokia	OK
8.3.3 ISO 20000-1	Service level management	check SLAs for Nokia and STC including serivce target availability more than 99.9% , and plan for future capacity for adding new projects (mobile towers) by Q3 2026 and Q2 2027	OK
8.3.4.1 ISO 20000-1	Supplier management \Management of external suppliers	Check contracts for supplier for Trio-application provider and related confideiality clauses and serivce availabiity and ticketing respond and emergency deployment.	OK
8.3.4.2 ISO 20000-1	Supplier management \ Management of internal suppliers and customers acting as a supplier	check internal supplier for procurement department acting as supplier.	OK
8.4.1 ISO 20000-1	Supply and demand \Budgeting and accounting for services	check with IT- Manager Group (Eng.Shadi) and Service delivery Manager for required assigned budget for expected capacity plan related to STC client SLA.	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.4.2 ISO 20000-1	Supply and demand \ Demand management	check STC SLA demand and focast for 2026 & 2027 this forcast till 2030.	OK
8.4.3 ISO 20000-1	Supply and demand \ Capacity management	check capacity related to bandwidth and expected hiring plans for covereing the client STC SLA for year 2026 till 2030.	OK
8.5.1.1 ISO 20000-1	Service design, build and transition \ Change management policy \ In-House Development Department	check change managment policy criteria for major and minor changes the related major changes related to any database changes and minors related to trio- application user interface change or update but not impact new processes.	OK
8.5.1.2 ISO 20000-1	Service design, build and transition \ Change management initiation\ In-House Development Department	change request done through emails and recommended to be upgraded to have ticketing system for better tracking for new services. check record for finicial department requirements for upgrading CRM.	OK
8.5.1.3 ISO 20000-1	Service design, build and transition \ Change management activities\ In-House Development Department	the Change management activities related to internal customer HR & serivce delivery for the CRM have been made through risk assessment to check the impact on other services and existing one.	OK
8.5.2.1 ISO 20000-1	Service design and transition\Plan new or changed services\ In-House Development Department	check xls sheet and trio-application planning for CRM upgrading related to SLA for the internal ciustomer and agreed deployment dates during June 2025	OK
8.5.2.2 ISO 20000-1	Service design and transition\Design\ In-House Development Department	check the documented design for MS-SQL database used for CRM and trio-application and also check the tracking system for developers and how the open source application works , using process flow using conditions for routing the program flow. Source code is secured inside database it self and inside trio-application with special previllages for IT useres (now only Shadi Al Tamimi have access to it A8.4 Access to source code). - Recommended for using MS-SQL to use coded tables and fields for more security of databases.(A8.28 Secure coding) - check the separate test environement VM for developvers and check the empty database used for testing and related risk (A8.31 Separation of development, test and production environments)	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.5.2.3 ISO 20000-1	Service design and transition\Build and transition\ In-House Development Department	check the builded software and database for updated CRM and related QC testing dated before deployment 15 days earlier by Eng. Tarek Salah and ensure that testing data is secured (A8.29 Security testing in development and acceptance) updating CMDB have been done.	OK
8.5.3 ISO 20000-1	Release and deployment management	Approved QC for CRM updated have the release 3.4 and deployed dated 17 june 2025.	OK
8.6.1 ISO 20000-1	Resolution and fulfilment \ Incident management	Check ticketing system for incident which categorize to major and minor and also have priority of responding to the ticket .	OK
8.6.2 ISO 20000-1	Resolution and fulfilment \ Service request management	the ticket system related to Trio-vendor but for internal customer require ticket send by emails. handling for requests with correction for events	OK
8.6.3 ISO 20000-1	Resolution and fulfilment \Problem management	if event (incident) require to be analyzed for root casue analysis RCA , to have corrective action , and known errors have been defined.	OK
8.7.1 ISO 20000-1	Service assurance \Service availability management	planned intervals (4 months), the risks to service availability shall be assessed to ensure availability - check risk assessment for Trio- CRM update SLA take into consideration relevant business requirements	OK
8.7.2 ISO 20000-1	Service assurance \ Service continuity management	planned intervals (4 months), the risks to service contnuity shall be assessed to ensure availability - check risk assessment for Trio- CRM update SLA take into consideration relevant business requirements	OK
8.7.3.1 ISO 20000-1	Information security management \Information security policy	check for backup , password and encryption polices.	OK
8.7.3.2 ISO 20000-1	Information security management \Information security controls	All security controls have been reviewed with IS risks (6.1)	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.7.3.3 ISO 20000-1	Information security management \ Information security incidents	security incident only related to review of Security Saudi Authority have been recorded and required to be closed , the authority review through online system.	OK
9.1.1	Monitoring, measurement, analysis and evaluation	- Check dashboard in Trio- Application for SLAs & compliance , bandwidth usages , resource usages and expected capacity for focast of capacity managment and plans . - Acheivment of targets by 83% for this year 2025 for achiving capacity plans .	OK
9.4 ISO 20000-1	Service reporting	- check dashboard service report for Tamkeen and CRM - All service reports can be devlopment from trio-application - Monthly report have been send to client and check service report for STC dated 02/12/2024.	OK
10.1	Improvement \Nonconformity and corrective action	check 3 NCRs for last internal audit and its closuer.	OK
			Not Applicable

Strength Point

- Top managment commetment for providing resources , and supporting and invovment of people in developing their managment system
- Using of Trio Application as develpment tools ,which can be modified by the In-House programming team.
- Good projects planning.
- Powerful datal log and dashboards.

Area for Improvement

- Recommended to use ISO 27005 as giude for risk managment and enable asset based and event based approach rathar than using ISO 31000 only.
- Recommended Implemntation of display desktop monitor screens for access controls devices logs rathar than using device log itself and USB SSD storage ,this to improve monitoring activities.(A7.4).

Observation

- SQL database and its tables it is recommended to be updated using a coding matrix techniques to enable more security to databases and its tables , instead of using predected names for tables like HR_table , or Emp_table which can be predected as human resource data in.
- Although the Access control devices are clock synchronized initially when connected , but recommended to always be sychncronized with all servers using same reference.

Minor NCR

NA

Major NCR

NA

Team Leader Recommendations

Recommeded to Grand the Certication for ISO 27001:2022 and ISO 20000-1:2018

Disclaimer Statement

The judgment of the management system is **based on the sample shown during the audit time.**

Lead Auditor Name:
Eng. Adel Belal

Signature