Audit Report

For

Advanced Operations Technology

Stage 2

Audit Dates: 03/11/2024 to 07/11/2024

Organization Details

Company:	Advanced Operations Technology
Address:	Khorais Rd, Riyadh- Saudi Arabia, P.O. 25904 Al Maadi 4, 151 Street , 11th Floor , Cairo- Egypt P.O. 11431
Contact Person:	Eng. Mohamed Abdelrahman
Email:	AOT@gmail.com
Audit Criteria:	ISO 27001:2013 / ISO 20000:2018
EA Code:	0
Scope:	Data Center infrastructure Solutions, Managed Support Service and Software Development 022365
No. of Sites:	1

Sites

Site Name	Location
Advanced Operations Technology	Al Maadi 4, 151 Street , 11th Floor , Cairo- Egypt P.O. 11431

Auditors

Auditor Name	Role
Adel Belal (AB)	Team Leader

Auditee Members

Auditee Name	Position
Mohamed Ezzat	InfoSec team leader
Yasser el okaby	Quality assurance & HR department
Hany Galal	Oracle ERP Support Manager
Sayed Boqari	BA / Weblogic Admin
Mohamed Abd El Rahman	Operation Manager & Managment Representative

No. of Man-Days
5.0

Audit Findings

Clause No.	Requirement\\Departement	Evidence	Result
4.1	Understanding the organization and its context	The organization determined external and internal issues that are relevant to its purpose Example of internal issues: - Lack of training - Lack of resources - Location moves - Work from home policy - Capacity management - Security issues Example of external issues: - Corona Virus - Change in KSA laws for labors. - Technology changing. - Internet speed change - Competition - hackers issues	OK
4.2	Understanding the needs and expectations of interested parties	The organization determined interested parties that are relevant to its purpose. And categorize them into (client , governmental , suppliers , outsourcing) The legal requirements AOT has to follow when implementing the services are the • requirements a addressed as per to ther service provided (shown in QM-S02 Legal&contractual agreements document updated on 26/4/2018) it shows list of legal agreements related to customers provided by AOT service and governed by these agreements such as (Cyber Security Framework ,Saudi Arabian Monetary Authority,Version 1.0,May 2017) • detail needs are written in supplier contract and customer SLAs • list of all legal and obligation requirements are mentioned in QM-S02 legal & contractual agreements. Example of interested parties and requirements : - AlwalNet (Supplier) contract start date 30/1/2011 , with SLA - Mobily (Supplier) Contract start date 12/08/2015, with SLA - Emirates NBD (customer) SLA start date 09/12/2016	OK

Clause No.	Requirement\\Departement	Evidence	Result
4.3	Determining the scope of the service management system	The scope of the SMS is documented with all defined services in (TM-F01 :AOT IT Service Management Plan , rev 1.1 dated 19/3/2020) and is called the AOT catalogue of services such as: • Software Application : Develop Java & .NET • Managed Services : o ERP Support Oracle o Third Party Application\services o Database o Hosting : ? Application ? System ? Network ? Security • ERP Solution : Oracle DB & Application • Business Intelligent : Analysis Reports • Datacenter infrastructure solution • Middleware: Oracle solutions • Share point • Support service : Outsourcing The Boudndary of providing the services is distributed in 2 locations : 1. Riyadh, KSA (All back-end operations such as data center, DBA administrations, Security, etc.) 2. Cairo, Egypt (front –end operations such as front office support, S/W development, Quality Control, etc.) Not applicable Clause form SOA is - A8.30 Outsourced development AS all software done inhouse only. SOA dated 10 DEC 2023 V.3	OK

Clause No.	Requirement\\Departement	Evidence	Result
4.4	Service management system	The management service process start with customer request send to Sales & Account Manager who classify the required services and send it to SLA manager \ Service delivery manager who prepare SLA and estimated offer , and prepare agreed SLA with interested parties and clients and send it back to sales & Account manager who will finalized the contract with the client. Then technical team start process after assigning a project manager , the team start with open CIs and after finish design and done with QC , the developing team issue first release which will be verified by SLA manager , if it ok , he will finalized the SLA for support and help desk will issue OLA with technical department for support ,and then the technical department will move the service to live environment by moving the service from develop server to production server , and then according to SLA the service delivery department will issue monthly service report to client. In case of any change or issue , the client will go to Itop application and open ticket and send it help desk if required new or changed service it will rout it to service delivery , if it concern about an incident like system failure it will rout it to technical support to analysis the root cause and solve it . AOT implement the ISMS in the scoped areas mentioned before (as mentioned in the clause 4.3) and shows in different areas of their procedures such as Information Security Management System Policy(SSN-P27) ,Risk Management Policy & Plan(SD-P04) and Risk assessment document (dated 23-3-2023)	OK

Clause No.	Requirement\\Departement	Evidence	Result
5.1	Leadership and commitment	-Top management leadership and commitment with respect to the ITSMS & ISMS identified and clearly mentioned through different ways such as AOT policy statement (TM-PS01) .issued issue 19/02/2020 , Rev 1. -Responsibilities such Service Owner and Service Manager. Where for each services, there is defined service owner responsibility , and to whom this offered service is provided . sample of the reviewed document is service catalgue (SD-F04) . -Services defined within AOT like data center infrastructure, Developing Software applications, managing services include (Hosting, oracle support and database management) -Also for the process owner a sample of process owner responsibility has been checked such as Service Level, Service Reporting, Availability Management, Service continuity management. -The management representative has beenassigned to Egypt branch manager with the letter dated 1/4/2018 with full responsibilities as required by the standard. - The Daily meeting with the head of mangementand other deprtmental heads has been reported by egypt branch head .most of meeting are verbal and actions to taken withinnext near period. It is found that The MR representative name (Mr. Mohamed Abdelrahman) is mentioned and attending in the management review meeting (TM-F03 dated 24/09/2024) as a Management representative on the behalf of the CEO. This management review meeting have been recorded by AOT online Zoom.	OK

Clause No.	Requirement\\Departement	Evidence	Result
5.2.1	Establishing the service management policy	AOT define an integrated ITSMS and ISMS policy , the policy is appropriate to AOT scope and include commitment for continual improvement , commitment for comply with legal and other requirements and provide high level of service quality to its client. AOT established ITSMS & ISMS policy issue 19/02/2020 , Rev 1 , with document no. TM-PS01	OK
5.2.2	Communicating the service management policy	AOT communicate the policy internally to all employees through trainings and workshops and to clients by attaching it in contracts and SLAs.	OK

Clause No.	Requirement\\Departement	Evidence	Result
5.3	Organizational roles, responsibilities and authorities	AOT determined roles and responsibility for all employees at all organization levels and during the audit samples for documented job description with defined roles and responsibilities are : - Capacity Manager , who has responsibility for ensuring that services and infrastructure are able to deliver the agreed capacity and performance targets in a cost effective and timely manner .and , He considers all resources required to deliver the service, and plans for short, medium and long term business requirements According to (SD-P02 Capacity Management Process) ,and address the business needs. - Problem Manager He could be defined as :One person (or, in larger organizations, a team) should be responsible for problem management. This problem admin is coordinating all problem management activities and is specifically responsible for: 1. Liaison with all problem resolution groups to accomplish quick solutions to problems within SLA targets. 2. ownership and protection of the Known Error Database 3. Formal closure of all problem records. 4. Liaison with vendors and other parties to ensure compliance with contractual obligations. 5. Managing, executing, documenting and planning all (follow-up) activities that relate to major problem reviews. 6. Problem Management process 7. Problem Report - Configuration Manager is responsible for maintaining information about Configuration Items required delivering IT services. To this end he maintains a logical model, containing the components of the IT infrastructure CIs(Configuration Item) and their associations According to (CO-P01 Configuration Management Procedure)	OK

Clause No.	Requirement\\Departement	Evidence	Result
6.1	Actions to address risks and opportunities	AOT determine the business risk related to ITSMS using the following Categories : - Risks impact on AOT as organization while it delivering services to customers , and this will include consideration of internal and external issues and legal requirements and information security requirements ., and this types of risks are pre-determined as fixed risks to organization fixed assets like their servers in data centers and information assets ..etc and reviewed periodically (normally every 3 months). - Risks impact on Client service due to customer requirements defined in SLA , and could affect other customers., and this type of risks are pre-defined in many phases (before commitment with client , during design phase while open CIs. And check the risk on other CIs. , Before deployment to check the risk of go live.) - They use matrix methodology for risk assessment 3x3 for likelihood and severity , with accept area green , treatment area yellow and avoid area red. - Sample of risk register : o Risk Scenario : Main DC electricity down o Vulnerability : UPS Failure , UPS limited capacity, Power Generator Not Started, UPS Inverter or stabilizer failure o Threat : Electricity outage , Electricity outage + Over load, PG Battery Died, Electricity surge or brownout - Sample of risk analysis : o Asset / Service : Primary DB Server o Risk Description : Server not responding o C.I.A Impact :A (availability). o Likelihood : 0.5 o Impact : 100 o Inherent Risk Value :50	OK

Clause No.	Requirement\\Departement	Evidence	Result
		o Existing Control : Local DG Server, Daily Backup, Daily Health Check and maintenance o Risk Owner : DC Operation	
6.2.1	Establish objectives	AOT establish objectives at different functions and levels for 2022/2023 Audit sample objectives are : Department : operational department Objectives : Reduce the average operation cost to 30% less than past year by end of 2021. Department : networking & System Security Objectives : To eliminate human mistake in the work environment and to decrease recovery time of the system to 10 min.	OK
6.2.2	Plan to achieve objectives	Department : operational department Action Plan : Reduce power consumption by servers consolidations , and replace the old servers with new servers with more power efficiency and enhance cooling system , and mitigate to visualization and cloud. Department : networking & System Security Action Plan : Educate SSN team for new technology and use automation to reduce human intervention and enhance security architecture.	OK

Clause No.	Requirement\\Departement	Evidence	Result
6.3	Plan the service management system	AOT establish service management plan (TM-F01 : AOT IT service mangement plan, rev 1.0 , dated 1/1/2018 and updated to rev. 1.2 dated 19/03/2023. Conatining the following : - AOT Service management Scope. - Objectives - Known limitation - List of Policies , Standards and regulatory requirements - Framework of authorities and responsibilities and process roles. - Authorities and responsibilities for plans, service management process and services - Human , technical, information and financial resources - Approach to be taken for work with other parties in design - Approach to be taken for interface service management process - Technology used to support SMS - Measurements of ITSMS effective - Improvement process - Change management process	OK

Clause No.	Requirement\\Departement	Evidence	Result
7.1	Resources	AOT top management determine and provide required resources for ITSMS & ISMS In Service Mangement Plan (TM-F01 : AOT IT service mangement plan, rev 1.2, dated 19/03/2023) have a reference for all AOT resources listed in asset register. During the audit sample : Checked for AOT data center which contain AOT DC HVAC system , AOT UPS 100KVA, AOT Power Generator, AOT DC Spare AC All equipment's are in good conditions , and check for it maintenance plans . The data center include servers for Backup Storage Server which under control of System Team Leader And checked Employee's Desktop/Laptop which provided for everyone and these devices controlled by Admin. Department.	OK
7.2	Competence	AOT determine the competency requirements for each job in Skill matrix and during the audit sample records for : Mr. Mohamed Abd Al Rahman he is Info. Systems and Security Manager and DC operation Manager the competency requied are Education Level : Universty Degree in Computer and Information Systems Skills & Qualification required : English, ITIL, Linux, windows administration, Networking, ISO/IEC 27001 Lead Auditor, Experience (Years) : over 10 years Mr. Mohamed Ezzat Ibrahim Morsy he is Bid Manager and Marketing Executive & Business Partner Manager Education Level : Universty Degree in Computer and Information Systems Skills & Qualification required : English, ITIL, Oracle Database 11g Sales	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Champion, Oracle Fusion Middleware Sales Champion, Microsoft certified Professional MCSD C# .NET Microsoft Certified Solution Developer, The 7 Habits of Highly Effective People – From Franklin Covey Middle East, E-Marketing Course (On Job Training), Boot camp Sales Training at Oracle, Soft Skills “7 Habits” (On Job Training), Soft Skills Course - Dale Carnegie Training Centre, Operating Systems: Windows, Programming Languages: C#, Microsoft Visual Studio, SQL Server, ASP.NET / Web Applications / Web Services, Web Parts, HTML, C# .NET Experience (Years) : over 5 years Performance appraisal and evaluation criteria are based on four parameters which are : Efficiency, Commitment, Cooperation, Quality focus And the action taken based on that criteria are : Under 60% : fail - Work under supervision & Training Required From 60% to 75% - Need Support – identified as Training Needs Greater than 75% - Acceptable and may be prompted. Part of Training Plan for 2024 was implemented due to Corona Virus and business crises, and this part is only for online courses provided by Google and Udemy for free.	
7.3	Awareness	Awareness for transfer to new standard ISO 20000-1:2018 relations with ISO 27001:2022, policy and objectives are made through AOT consultation company QI , which provide online zoom awareness to AOT employees in four sessions in MAR , MAY , AUG and OCT 2020	OK

Clause No.	Requirement\\Departement	Evidence	Result
7.4	Communication	AOT communication have two ways : 1- For internal communications this done through emails and regular Sunday zoom meetings , and in this communication they discuss all business and service aspects. 2- External Communications with clients through Emails and through Itop by arising a ticket " open ticket " which converted by help desk to Change request This defined in communication procedure SD-P02	OK
7.5.1	General	All documents are saved in Document Management system DMS .It is an open source application rev 2.0 with the updated version called QMD application on server , this application have all updated documents and records , and one a document is uploaded to the system this mean that it is a controlled document. XLS sheet called master list and distribution list of SMS documents is attached to DMS show all documents and records used in AOT ITSMS & ISMS.	OK
7.5.2	Creating and updating documented information	AOT has document control process for creating and updating documents the document & Record control procedure is available QM-P02 rev.2 is uploaded on DMS. Coding system is used for documents are QM-S01 Coding System.	OK

Clause No.	Requirement\\Departement	Evidence	Result
7.5.3	Control of documented information	All controls are through uploaded on DMS , any document is not uploaded on DMS this mean that is not controlled and not allowed to be used . All records including SLA are uploaded in DMS also in latest version According to users privileges , each user can access some documents and this is determined by Document controller Mr.Yasser , according to each employee job description . All risks related to employee accessing documents are identified and addressed in risk register for ISMS in accordance with Annex A.	OK
7.5.4	Service management system documented information	All documented information are listed in Master list of document and updated in DMS Master list contain up to 95 documents and records and table divided into 4 columns (serial , Document name , Code , Rev. No) Example : (89 – AOT Data center Visitor Registration Log – SSN-F06 – Rev.2.0) (82 – Information security controls & objectives – SSN-S02 – rev.2.1) (47 – Operating Level Agreement OLA – SD-F02 – rev 1.0) (41- Risk management Policy & plan – SD-P04 – rev 2.1) (42- service continuity & availability management process – SD-P05 – REV 1.0) (45- ITSM Improvement policy SD-P08 –rev 1.0)	OK
7.6	Knowledge	AOT register all necessary knowledge and experience in system called lesson learning , this done now using zoom meeting and they register the information in the video discussions.	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.1	Operational planning and control	AOT implement controls for service delivery that have been identify its risk and assign risk assessment for it , and during the audit sample Risks of System operations: Threats : Backup Storage server unavailable Risk Treatment Action : Copy Archived data to removable offline media (media is available in hard drives) Responsibility by : System Operation Threats : Local Vulnerability Exploits (L-BOF) Risk Treatment Action : Install AV, Kernel Hardening , User Policy , Vulnerability management, Patch management. Responsibility by :security team Risks of Application team Threats : e-Trade Application Server failure Risk Treatment Action : Transfer to e-Trade DR Responsibility by : application - NOC teams Risks of DB operations : Threats : Database file corruption Risk Treatment Action: Systems team check logs daily to know if there are any corruption on the disk and do immediate File System check if found any. Responsibility by : DBA and Systems teams Threats : privilege user account locked Risk Treatment Action : Daily DB Health Check performed before production hours. Check Alert.log file daily. ,and Continuous monitoring of the DB through Enterprise Manager/Grid Control monitoring systems. Responsibility by : DBA Risks of Network operations : Threats : Primary link to Tadawul is down Risk Treatment Action : Switch to DR datacenter	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Responsibility by : NOC Threats : Juniper firewall is down Risk Treatment Action : Switch to Linux Firewall Responsibility by : Security & NOC & Systems	
8.2.1	Service delivery	AOT establish Service management Plan SMP , and define all services categories in the scope of ITSMS with reference to details services in service catalogue. SMP contain all resource categories with reference to asset register	OK
8.2.2	Plan the services	AOT is have planned for its services and give the priorities for service delivery and action taken these have been checked through application used for creating the service request and change request in Itop ,which define the priority based on the methodology defined in SMP	OK
8.2.3	Control of parties involved in the service lifecycle	All parties involved in service life cycle for AOT have determined as interested parties and have been controlled through SLA and contracts Sample contract for supplier "MobileWeb" these contract define the following topics: - Service level - Support - Availability - Target response times & target maximum fix time - Network reach - Refund conditions	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.2.4	Service catalogue management	AOT establish a service catalogue that updated regularly as any service updated or changed or removed Service catalogue contain main topics : - Service main Category (Example checked - Software development) - Service Sub Category (Example checked – ADF&JAVA Development , .NET development) - Service Sub-Sub Category (Example checked inside ADF&JAVA Development there are software design , Software support, medan) - Description (Example checked " Internal and external service ") - Limitation & Constrains (Oracle ADF web development) - Technical Specification (Example checked for SharePoint "allows for storage ,retrival ,searching archiving, tracking ..etc.) - Hardware requirements (Example checked for SharePoint RAM 16 GB , 64bit, 4 Cores , 250GB hard disk) - Software requirements (Example checked for SharePoint 64 bit SQL-server , windows server 2012 R2 , visual studio 2015 - Human resource requirements (Example checked for SharePoint 4)	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.2.5	Asset management	AOT define asset register containing all its assets including information assets and financial assets During audit sample : Asset : AOT DC Category : Data Center Asset Owner : DC Manager Asset : ENBDC DB Server Category : Primary DB Server Asset Owner : DBA Manager , Apps DBA Manager Asset : ENBDC SYSLOG Server Category : SYSlog / NTP server/SMS GW/SMTP Asset Owner : System Team Leader Asset : AOT Firewall , ENBDC Firewall Server Category : Firewall Asset Owner : Security Team Leader	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.2.6	Configuration management	IT department establish a documented procedure to consider the configuration management found in DMS (CO-P01: Configuration Management Procedure , rev 2.2 dated 1/1/2018) The procedure contains - configuration management policy - configuration managemnegt process - workflow - responsibilities matrix - KPIs and governance. It is reflected on configuration manager module in ITOP as it is linked to the CI dbase . The confirguration management database CMDB have been found in Itop application with all CIs. And regular daily backup for CMDB have been stored in AOT storage 2 in Backup server and another copy offline stored in hard drive weekly. All storage offline media (hard drives and DVDs) are stored in locker with password	OK
8.3.1	Relationship and agreement \ General	AOT determine the key suppliers and have a contract with each one of them and ensure that any supplier have a sub-supplier have a documented agreement with him.	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.3.2	Business relationship management	AOT assign a contact person for each customer these person should have customer feedback and coordinate any requirements for client to AOT. AOT check the performance to service delivery to customer monthly through the monthly report During the audit sample checked Service level Report for client Emirate NBDC (SD-F03) dated September 2020. And this show for total service availability (target >=99.99% and achieved 100%) And show for Client respond Time (target >=99.99% and achieved 100%) And show for Completion of EOD Archiving (target <6 hrs. and achieved 19 min.)	OK
8.3.3	Service level management	AOT have established with each customer SLA for agreed service delivery and performance including reporting system. During Audit sample SLA for client Emirate NBDC (renewal SLA) this SLA include service delivered and service targets and performance and reporting The SLA have been approved and signed by both sides.	OK
8.3.4	Supplier management	Supplier Contracts have been examined during the audit for MobileWeb Supplier Contract define the following items : - Service level - Support - Availability - Target response times & target maximum fix time - Network reach - Refund conditions These items include the responsibility & Authorities for both sides	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.4.1	Budgeting and accounting for services	Process Description: AOT has established a documented policy and procedures on budgeting and financial planning for the expected or ongoing supported services(FI-P01: IT Service Budgeting& Accounting,rev1.2 dated 1/1/2020). The procedures describe the policy for establishing the budget, process flow, roles and responsibilities and the key governance. AOT established the budget on yearly basis and refereing it mainly to a fiscal year conecpt (begian 1st of April and End on 31st of March). AOT determined the sources for budget estimation based on some sources such as (Business unit sub-budgets, activities budgets, new planned services budgets, sales sections budgets and plans, historical expenditures for the last 3 fiscal years, sales targets, etc...) there is no exact budget for each department clearly determined as it is linked to the potential projects forecast with customers. However, the Departments heads as well as the top management committed to ensure the enhancement of the ITSMS as per customers' requirement Evidance : Budget assign for Calender year 2024 for upgrading AOT data center servers , for cyber Security trainings ,and for PECB recertification for ISMS & ITSMS this all shown in management review dated 24/09/2024.	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.4.2	Demand management	AOT have analysis the services demands each 6 months and report for allocating funds in management review , this include forecast customer needs , supports and capacity management and workload trend. During audit sample show in management review the allocation of budget related to client ENBDC managed service requirements.	OK
8.4.3	Capacity management	During audit sample for capacity management for customer ENBDC report dated October 2023(SD-F01) Which contain the following topics : - Purpose - Scope - Formal changes & opened CRs required for capacity - Technical indications and symptoms of the current capacity performance (for system and servers) o Utlization Alanlysis o Upgards required/recommended to enhance the capacity - Technical indications and symptoms of network current capacity performance	OK
8.5.1	Change management	AOT established a change management procedure docuemnted in (CO-P02: Change Management Process , rev 2.2 dated 19/3/2020). The procedure consists of change management policy, workflow, models of change management, key activities, responsibilities matrix, KPIs, input and output as well as dependencies and control governance. Process schematic diagrams for change management are : • 11.1. ITOP - Internal & External change requests • 11.2 ITOP - Ticketing cycle of user requests (As a trigger for Change /	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Incident) • 11.3. ITOP- ticketing map • 11.4. Normal & Emergency Change Lifecycle. Audit Sample for customer ENBDC , for change request C-014660 for restart DB and weblogic servers. This action done by AOT system team as part of preventive maintenance to the system This impacted to production weblogic & DB will down during action Plan for restart monthly is : - Stop Web logic servers (nageswar) - Shutdown database servers (mafaz). - Restart servers (system team) - Start database servers (mafaz). - Start Web logic servers (nageswar) - Health check by support etarde is running and accepable (sysytem team) - Email notification to customer that restart is done (support team). - Customer test from his side (mohamed saleh) Production servers : 192.168.42.1 database server 192.168.41.10 weblogic server Emergency change also checked for change request C-014653 for same client The request is Block 185.112.157.178 And reson for change is Malicious IP and it imapct rule will not work The action is to scan IPs from 185.112.157 to 86.51.12.156 and block 185.112.157.178 , this IP is listed as a black llisted as this try to hack the firewall , and this action done by security engineer and this added to firewall juniper (ENBDCPR) The CR- created 2023-10-25 09:27:57 and closed 2023-10-25 09:49:30. , this action appear in oct 2023 monthly report.	

Clause No.	Requirement\\Departement	Evidence	Result
8.5.2	Service design and transition	Process Description Design is initiated by change management policy if major change have been made Change management process (CO-P02: Change Management Process , rev 2.2 dated 19/3/2020). Which contain the policy of major change that lead to design & development process . AOT infrastructure datacenter design The schematic diagram of the planning was reviewed includes AOT DC connected to AOT –EGY and AOT-DC Awlnet Audit sample a details for AOT–DC in KSA For AOT-DC contains - DMZ SW1 & DMZ SW2 which connected to DB zone & Application zone and webzone - These switches connected to internet through a juniper firewall and connected to backup router and production router - AOT floors users are connected through Access F1 sw1 , Access F2 sw1, Access F2 sw2, Access F3 sw1, Access F3 sw3, Access F4 sw1 , with access points.	OK
8.5.3	Release and deployment management	Process Description : AOT have a release management process RS-P01 this process to : - Ensure that only approved and correctly identified and configured items are released to the production environment. - To ensure that only authorized, correct versions of software are released into the production environment. - To optimize control and understanding of the Release Management process as well as to create a clear audit trail to	OK

Clause No.	Requirement\\Departement	Evidence	Result
		assess the effectiveness of the Release Plan, and help ensure a successful Release. - Testing is required to ensure the Release meets all expectations and does not create any change related incidents. - Optimize the benefits of the Release process. - Consistent versioning and naming of IT assets is critical to establishing control of the infrastructure and ensuring that only the authorized and correct versions of software and hardware are installed into the live environment. - To ensure that service can be restored with minimal impact on the business in the event of failure of the Release. - To enable the Release of defined Release units about which knowledge is available to determine and reduce risk of change related incidents. - To reduce the risk of change related incidents by thorough documentation and understanding of possible impacts and to facilitate the appropriate testing relative to those risks. - This policy will ensure that all of the necessary steps in testing the Release and ensuring that the production environment is prepared to accept the Release with no disruptions to the business. - To standardize the Release Build procedures across the enterprise and gain more control through the use of documented repeatable and proven procedures. - To ensure that all Releases are planned according to the Release Policy and that no releases are implemented without following the Release Management process. - All Releases must be thoroughly tested; in addition audits of the	

Clause No.	Requirement\\Departement	Evidence	Result
		infrastructure are required to assure environmental readiness; non-technical matters such as training and user acceptance with the release are also important considerations. And this procedure apply to : - Includes all Releases of the new or changed managed services of DC clients. - Applies to all infrastructures Configuration Items (CIs) within the scope of Change Management. - All Software applications that are within the scope of change management including software supplied by external vendors. - All Releases will be tested as required by the Change Management process. - All Releases that are required by the Change Management process. - This policy applies to all components within the scope of Configuration Management. - Includes all Releases under the control of Release Management. - All software and hardware CIs within the scope of change management. Use a release policy RS-P01 Release Management policy and Release plan and release test Emergency release agreement is part of SLA define the Emergency cases for release and deployment The tests & measurements should consider all potential impacts on business according to the BIA (Business Impact Analysis) as per included in the BCP	
8.6.1	Incident management	This process handled and records in Itop and in form RN-F01 During the audit sample for incident No : I-01041 Client : OBIC	OK

Clause No.	Requirement\\Departement	Evidence	Result
		Incident Title: OBIC SMS not working Availability Impact: AOT side Summary of Incident description & symptoms: The SMS Service wasn't working Successfully List of Services / elements affected: SMS. Business Impact: Customer didn't receive SMS. Incident resolution & actions taken with major steps: Customer complained that he is receiving SMS twice on @ 8:36 AM KSA. - We checked and found that our technical team ran the alert task on prod server in parallel with running task on backup server. - We shut down the service on backup server and ran the one on prod only @ 9:00 AM KSA then customer confirmed that he is receiving the SMS once. - Customer complained that he isn't receiving the SMS on @ 8:30 AM KSA. - We checked and ran the task manually @ 8:55 AM KSA and he received the SMS successfully. - Customer complained that he isn't receiving the SMS on @ 8:35 AM KSA. - We checked and ran the task manually @ 8:55 AM KSA and he received the SMS successfully. Root Cause Analysis: - For issue 1 our technical team ran the task from prod in parallel with running the task on backup". - For issue 2 the tool which runs the task automatically wasn't installed. Other Key Action Items and follow-up Required (if any): Make sure that there is only one task running and this tool is installed.	

Clause No.	Requirement\\Departement	Evidence	Result
8.6.2	Service request management	During the audit the sample for a service request for client ENBDC No: C-014502 The client opens a ticket for that request asking for upgrade RAM memory for AMQ & PS on fox server. This request impact for applications The request description is that "We need to knew the maximum Java heap configured for FOX 192.168.47.1, we are going to upgrade the RAM today to 32 GB. Fallback plan: java not supports to allocate more than 1GB on 32bit operating system .it support more than 1 GB in 64 bit operating system. Also check for a new service request for : Client : ENBDC Request No : R-014260 Dated : 21-07-2020 Title : PTTP FTP Connectivity Parameters Service Type : Managed Service Package 1 Product : UAT Request details : To enable reaching Tadawul FTP server from UAT server (192.168.45.10) as per details	OK
8.6.3	Problem management	For the problem management AOT establish a documented procedure for problem management considered in DMS(RN-P01 Problem Management Process, rev 2.2 , dated 19/03/2020). The procedure contains problem management policy, workflow, roles and responsibilities matrix, KPIs and governance. Workflow shows how to identify the problem, recording, priority, update, escalation resolution and closer. During the audit a problem was invistigated and traced through ITOP application	OK

Clause No.	Requirement\\Departement	Evidence	Result
8.7.1	Service availability management	AOT establish and document service availability process and plans Service /business availability / continuity process SD-P03 Purpose of process is : • Fulfillment of the agreed service levels. • Reduction in the costs associated with a given level of availability. • The customer perceives a better quality of service. • The levels of availability progressively increase. • The number of incidents is reduced.	OK
8.7.2	Service continuity management	During the audit sample checked plans for client ENBDC done in april 2023 For Business continuity & Disaster Recovery plan SD-P05 The BCP is contain the following items: - Distribution - Purpose - Scope of application - Abbreviations / Terms / Definitions - Responsibility - Inputs - Outputs - BCP / DR Planning process o Introduction& communication details o Business Continuity Planning Process o Communication (having communication list with names,address, email , mobile no.) for team members , vendors , managers o Facility Requirements o Infrastructure requirements o Alternate locations: o Equipment Requirements: List workstations, phones, phones, copiers, and requirements for set up o Software/System Application Requirements o System Description and Architecture & Server IP’s (update with murabha Diagram)	OK

Clause No.	Requirement\\Departement	Evidence	Result
		o Prevention Phase: Risk Management planning (include risk register with priprity and action to be taken) - Business Impact Analysis - Pre-disaster Activities - List the tasks that are required on an ongoing basis, to keep the plan current and viable and indicate the person assigned to complete - Preventative activities - BCP / DRP test & validation - BCP / DRP training / awareness: - Response Phase : Business continuity and Disaster recovery Scenarios Checked scenario for - Primary internet connection is down (no connectivity) - Primary router at PR site is down	

Clause No.	Requirement\\Departement	Evidence	Result
8.7.3	Information security management	AOT integrate ITSMS with ISMS during all work activities during providing its services And all controls for reducing risk have Annex reference from SOA in ISMS. During the audit checked Asset : Backup Storage Server (located in AOT-DC in KSA) Risk Description : Server not responding C.I.A Impact : A (availability Impact) Existing Control : Copy Archived data to removable offline media and Daily Health Check maintenance SOA control : A.11.2.4, A.17.2.1 Risk Owner : DC Operation Asset : Backup Storage Server (located in AOT-DC in KSA) Risk Description : Unauthorized Access C.I.A Impact : C.I (confidentiality & Integrity Impact) Existing Control : Firewall, Network Segment, Access Control Policy, backup encryption SOA control : A. 5.1, A.6.1.2 , A.11.2.1, A.12.1.4, A.18.1.3 Risk Owner : DC Operation	OK
9.1	Monitoring, measurement, analysis and evaluation	AOT monitor performance for its service monthly and Quarterly for its clients During the audit checked the following reports: - ENBDC Capacity Report October 2023 Quarterly - ENBDC Security Report October 2023 Quarterly - ENBDC service Report September 2023 monthly - SFC service Report August 2023 monthly	OK

Clause No.	Requirement\\Departement	Evidence	Result
9.2	Internal audit	Internal Audit procedure QM-P02 AOT define audit program with audit frequency considering process importance and status. Due to Corona-Virus all audits will done online as AOT have policy work from home in all 2020. Last internal audit dated : 22/08/2024 Audit criteria : ISO 20000-1:2018 & ISO 27001:2022 Audit Scope : AOT Service scope defined in SMP Audit method : Online using Zoom Audit result with 2 NCRs related to updated data in DMS	OK

Clause No.	Requirement\\Departement	Evidence	Result
9.3	Management review	Audit sample reports for : Client : Saudi Finance Company SD-F03 Report Type : Monthly Report Aug.2023 This report prepared by Eng. Mahmoud Sobhy ,Service delivery department Report contains: - Utilization graphs - DB and applications status report - Production security application utilization - Change management - Event log review - Vulnerability assessment and patch management - Incidents - Firewall review report - Information security report review o Early notification alert o Incidents/error required patch/bug fixes Client : ENBDC Report Type : security & Vulnerability assessment report SSN-F10 dated Oct 2020 Prepared by : Hazem osama , Operation department Report contains : - Purpose - Scope - Security report and description - Vulnerability assessment from inside servers - Vulnerability scan for public IPs - Early notification alert - Incidents/error required patch/bug fixes - Firewall review report - Summary of reports review - Software installed review - Physical security review	OK

Clause No.	Requirement\\Departement	Evidence	Result
10.1	Nonconformity and corrective action	Corrective action sampled in audit for NCR #1 raised from internal audit dated 22/08/2024 related to DMS updated data Root cause analysis have been done , which is due to delay respond due to corona virus for responsible person in charge .	OK
10.2	Continual improvement	AOT shows its commitment to continual improvement of providing ITSMS & ISMS in service management process this is shown from AOT policy and AOT statement (TM-PS01) which indicated its scope of service provided to customers, with commitment to fulfill customer requirements as a part of its objectives to exceed customers' expectations, ITSMS & ISMS requirements as well as regulatory and statuary requirements.	OK

Clause No.	Requirement\\Departement	Evidence	Result
Documents	List of documents included in the audited MS	- Service Management System Plan - SD-F03 Service Report - Management review (Minutes of meeting) - Service Management Policy - Service Reporting Procedure - Communication Procedure - Job Description(Filled for all category) - Process chart - Assets Register - AOT I TSMS process map - Procedure for document & Record control - Skills Matrix Sheet - Procedure for internal audit - Change Management Policy - Customer Service Report - Design and Transition of New or Changed Services Process - Operational Level Agreement Template - Service catalogue - Service level agreement - Service Reporting - Customer Complaint Report - Procedure for service continuity - Service Continuity Testing - Risk Management - Procedure for availability management - Risk Management And Tracking Sheet - Business Continuity Test Report (BCP / failover test results) - Budgeting and Accounting Policy - Procedure for Capacity Management - Capacity Management Policy - Capacity Planning - Risk Management And Tracking Sheet security - Information Security Policy - Visitor Policy - E-mail and messenger use - Visitor Entry Register	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.1	Policies for information security	SSN-P27 Information Security Management System Policy documents (Revision No. : 2.1 | Revision Date: 30/4/2023)	OK
A5.2	Information security roles and responsibilities	Identified in service catalogue document (SD-F04, dated 4/4/2018)	OK
A5.3	Segregation of duties	Checked through personnel interviewed and documented in service catalogue document (SD-F04, dated 4/4/2018)	OK
A5.4	Management responsibilities	Example checked is Job description of Mr. Alaa Helala(Security team leader-KSA) : he was interviewed within the auditing process and his job description (HR –F04) was clearly shows his roles and responsibilities	OK
A5.5	Contact with authorities	Identified as reviewed for Mr. Mohamed Abdel Rahman (OP manager) handling Tadawul(KSA Financial exchange) and made the agreement with them (Tadawul Member Security Standard For Electronic Trading (E-Trading) Version 2.2)	OK
A5.6	Contact with special interest groups	Such as suppliers (Identified in service catalogue document (SD-F04, dated 4/4/2018)	OK
A5.7	Threat intelligence	-	OK
A5.8	Information security in project management	(Identified in service catalogue document (SD-F04, dated 4/4/2018)	OK
A6.1	Screening	Controlled by the document (HR-P01: HR procedures) which shows qualifications , background(legal(through criminal act clearance certifications) and professional through technical certifications of each employee)	OK

Clause No.	Requirement\\Departement	Evidence	Result
A6.2	Terms and conditions of employment	Through contract of supplier (SAMA: Cyber Security Framework Saudi Arabian Monetary Authority , Version 1.0 ,May 2017) and mentioned clearly in (clause 1.5 Responsibilities: "The framework is mandated by SAMA. SAMA is the owner and is responsible for periodically updating the Framework.")(SAMA established a Cyber Security Framework ("the Framework") to enable Financial Institutions affiliated with SAMA ("the Member Organizations") to effectively identify and address risks related to cyber security. To maintain the protection of information assets and online services, the Member Organizations must adopt the Framework)	OK
A6.3	Information security awareness, education and training	As an example (Physical Security and physical Access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018) was communicated through email dated Feb, 2018.	OK
A6.4	Disciplinary process	Reviewed through Mr. Alaa Helala contract clause of contract termination and matrix of stages of disciplinary actions to be taken in case of security breach performed by employee	OK
A6.5	Responsibilities aftertermination or change of employment	Reviewed through Mr. Alaa Helalacontract clause of contract termination and matrix of stages of disciplinary actions to be taken in case of security breach performed by employee	OK
A6.7	Remote working	Shown –as in clause 6.2.1- in document : SSN-P03 Physical Security and Access Control Policy updated v1(rev 2.1 dated 1/1/2018) (Clause 2.0 Scope of Application)	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.9	Inventory of information and other associated assets	It was reviewed through ITOP application and the link between the assets and the provided service through this particular asset is shown clearly through ITOP (Example :change management process and service provided to customers)(sample : GEA service request , date 18/6/2019 , change request ID: C-012768)	OK
A5.10	Acceptable use of information and other associated assets	As an example Shown within (SSN-F01 :Data center authorized access list review, Rev 2.1 ,dated 1/1/2018)and (TM-F01: AOT service management plan)	OK
A5.11	Return of assets	Shown within Murabha SLA agreement (Rev 1.0 Date 8-02-2015) showing SLA contract termination terms and deliverables upon termination	OK
A5.12	Classification of information	Reviewed through document (SSN-P27:Information classification Policy, Rev 2.1, dated 1/1/2018)	OK
A5.13	Labelling of information	it shows a table of information classification and labeling (pages 4,5, and 6)	OK
A5.15	Access control	Evidence SSN-F01 :Data center authorized access list review, Rev 2.1 ,dated 27/11/2018) which show it is updatd by removing MrEzzat ‘s name and replaced with MrHelala as the new security head .And (TM-F01: AOT service management plan) As per to AOT operation manager, it is shown within audit the access list to AOT resources governed by :Networks and communications security policy(SSN-P02, Rev2.1, dated 1/1/2018)	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.18	Access rights	All user access management is governed by users physical and logical policies the 2 files: -Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018 -Logical system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018 identify all AOT users access management	OK
A5.17	Authentication information	Shown in document : High privileged account usage policy & procedure:SSN–P16 rev 2.1, dated 1/1/2018 . it shows the access management is controlled such as Admin/Root password access as it is divided in 2 physical offices (clause : 7.3. Password protection)	OK
A8.24	Use of cryptography	Shown in: - Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018 clause :7.3 Secure Area Policy, SUB Clasue:7.3.5 - NCSP policy:SSN-P02, Rev2.1, dated 1/1/2018) Clauses :7.2 WAP and 7.2.6 Public Networks and 3rd-party Networks Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018) Clause :2.3.2 Security of connections and networking traffic	OK
A7.1	Physical security perimeters	It is governed through Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 27/11/2018	OK
A7.2	Physical entry	It is shown within controlled document : SSN-F01(:Data center authorized access list review, Rev 2.1 ,dated 27/11/2018)	OK

Clause No.	Requirement\\Departement	Evidence	Result
A7.3	Securing offices, rooms and facilities	It is stated clearly within audit interview and site visit for both sites under the scope of auditing and showed the access control to both building facilities in KSA and Egypt	OK
A7.5	Protecting against physical and environmental threats	It is checked within site visit how the protection applied in both site such as firefighting system (FM200) and a copy of supported service report to facility generator and fire system	OK
A7.6	Working in secure areas	It is checked and shown in Data center in KSA site and how the access of assets is controlled governed by applied policy shown in document : Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018 clause :7.2 physical Access control Policy It is checked within site visit to Data center in KSA site how the room designed and the entry is a sliding structure for loading/unloading any equipments or IT assets(such as racks, servers, COMM equipments , etc..)	OK
A7.8	Equipment siting and protection	Shown in auditing site visit and air conditioning design in data center(such as AC tunnel design) and operation team department (such as central AC environment and centralized facility fire system)	OK
A7.11	Supporting utilities	Shown within site visit the UPS room(UPS power 100 KVA -4 redundant units) which is separated from the data center room and provide power if power failure incident arises.	OK
A7.12	Cabling security	All shown is well truncated in the structural designed building and inside data center under the raised floor .	OK
A7.13	Equipment maintenance	Indicated clearly from the man in charge and shown within maintenance service report :Supplier (SETRA) dated 8/1/2018 to power generator .	OK

Clause No.	Requirement\\Departement	Evidence	Result
A7.14	Secure disposal or re-use of equipment	It is checked within maintenance policy shown in file :SSN-P28 Preventative Maintenance Policy and procedures, Rev 1.0 dated 1/1/2018 and it indicates how to control and manage the process of H/W equipments or S/W assets replacement or reinstalled	OK
A7.9	Security of assets off-premises	Shown in :SSN-S02 Information Security Controls_ Objectives file document and shows how to control security of IT equipments	OK
A5.37	Documented operating procedures	It is checked from the documents: - TM-PS01 AOT ITSM_Policy - TM-F01 AOT IT Service Management Plan	OK
A8.6	Capacity management	Available in document :SD-P01 Capacity Management Process , rev1.0 , dated 1/1/2018	OK
A8.31	Separation of development, test and production environments	It is done as it is found that the development team is located in EGYPT Office , Cairo and the operation team is located in KSA with all operational environment (such as data center)	OK
A8.7	Protection against malware	It is controlled through policy document :SSN-P06 AntiVirus, AntiMalware,Anti-Trojanand Personal Firewalls Policy, rev 2.1 , dated 1/1/2018) and it is communicated through email message sent from the EX security team leader (Mr. Mohamed Ezzat) to all users dated 2/3/2015 pointing that on how to use application ITOP to open ticket with any incident regarding malware message arises	OK
A8.13	Information backup	It is reviewed from the document checked :SSN-P21 Backup RecoveryPolicy_2.2, rev .2.3 dated 1/1/2018 and showed the control actions used for backup process	OK

Clause No.	Requirement\\Departement	Evidence	Result
A8.15	Logging	Shown within documents :SSN-P13 Event Logging Procedures, rev 2.1 , dated 1/1/2018	OK
A8.17	Clock synchronization	It is used automatic clocking settings and related to the time zone (Cairo +2:00 hrs)	OK
A8.19	Installation of software on operational systems	Reviewed from document : Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018) Clause :2.6.2 Software design and development	OK
A8.8	Management of technical vulnerabilities	It is addressed in AOT Risk assessment file (Dated 23/4/2018) and the control taken is :Periodically Vulnerability assessment, Patch management and this reduce the risk factor from 100 to 25 (under calculation of AOT risk matrix)	OK
A8.20	Networks security	Governed and controlled through policy file : SSN– 02 Networks and communications security policy, rev 2.1 , dated 1/1/2018	OK
A8.21	Security of network services	Shown in different evidences such as : - SSN – 02 Networks and communications security policy, rev 2.1 , dated 1/1/2018 - Catalogue of service document (SD-F06) - SD-P04 Risk Management Policy & Plan - SFC SLA dated 2017And reflected to service report sample :SFCMonthly Service Report-May-2013	OK
A8.22	Segregation of networks	- All AOT customers have a dedicated N/W environment and it clearly mentioned in their SLAs such as :SFC SLA dated 2017.	OK

Clause No.	Requirement\\Departement	Evidence	Result
A6.6	Confidentiality or non-disclosure agreements	It is reviewed through contract agreement samples such as form (Mr. Alaa Helala) with his confirmed signature	OK
A5.14	Information transfer	- It is reflected as a proof from an incident report RN-F01 and shows how a diversion of traffic done through AOT RD site (incident ID: I-011043 dated 26/9/2017)and controlled through Murabha SLA dated 2015, final version dated 28-02-2015 -Interested parties such as GO on behalf of AOT customer Tadawul and the SLA shows the scope of work indicating information transfer through GO network . -Email system is protected through VPN connectivity as mentioned on more than a documents such as : - SSN – 02 Networks and communications security policy, rev 2.1 , dated 1/1/2018 - Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018	OK
A8.30	Outsourced development	N/A as all software done in house	Not Applicable
A8.33	Test information	It is shown through process of development documents : - SD-P03 Design And Transition Of New Or Changed Services Process , rev1.0 , dated 1/1/2018 - RS-F01 Release Management & release acceptance Plan-Initial revision , rev 1.0 , dated 1/1/2018	OK
A8.27	Secure system architecture and engineering principles	Information Security Management System Policy SSN-P27	OK

Clause No.	Requirement\\Departement	Evidence	Result
A8.29	Security testing in development and acceptance	It is shown through process of development documents : - SD-P03 Design And Transition Of New Or Changed Services Process , rev1.0 , dated 1/1/12018 - RS-F01 Release Management & release acceptance Plan-Initial revision , rev 1.0 , dated 1/1/2018	OK
A5.28	Collection of evidence	This is done through ITOP (service management application program) and DMS (Document management application program)	OK
A5.27	Learning from information security incidents	In the risk assessment file and ITOP application program used for service management it shows a classification of incidents and how the corrective actions taken and shown in a process such as (Corrective/Preventive action Procedure document QM-P03, rev 1.1, dated 1/1/2018)	OK
A5.26	Response to information security incidents	Suppliers: are covered through SLA agreements, example such as communication links service provider (GO) with its SLA (Rev -2015) which is providing communication service to AOT Customer (Murabha)..this is reflected in service report(SD-F03, June,2023) with incident ID: I-009751 (Murabaha GO IP VPN link is down) and it is closed ref to GO feedback (mentioned in detail in the report clause 2.1 incident log) and shows the utilization measurements	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.25	Assessment and decision on in formation security events	Suppliers: are covered through SLA agreements, example such as communication links service provider (GO) with its SLA (Rev -2015) which is providing communication service to AOT Customer (Murabha)..this is reflected in service report(SD-F03, June,2023) with incident ID: I-009751 (Murabaha GO IP VPN link is down) and it is closed ref to GO feedback (mentioned in detail in the report clause 2.1 incident log) and shows the utilization measurements	OK
A5.30	ICT readiness for business continuity	Indicated in document (SD-P05 Service Continuity And Availability Management Process) and show the result through document (SD-F05 BCPFailoverTestResults)	OK
A5.29	Information security during disruption	Indicated in document (SD-P05 Service Continuity And Availability Management Process) and show the result through document (SD-F05 BCPFailoverTestResults)	OK
A8.14	Redundancy of information processing facilities	AOT has stated within interview and show schematic diagrams of operational site and it has 1 main production site in Riyadh and another 2 DR site (semi on/semi off) covering all service provided by AOT to all related parties such as customers, employees and suppliers as well	OK
A5.31	Legal, statutory, regulatory and contractual requirements	It is mentioned and showed evidence of contractual agreements ref to customer requirements such as (E-Trading system minimum security requirement) and it is applied to customer (Tadawul) through document (Tadawul Members Security Standard for E-Trading 2.2_Updated)	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.32	Intellectual property rights	It is mentioned and showed evidence of contractual agreements ref to customer requirements such as (E-Trading system minimum security requirement) and it is applied to customer (Tadawul) through document (Tadawul Members Security Standard for E-Trading 2.2_Updated)	OK
A5.33	Protection of records	This is shown in : - (Physical Security and physical Access Control Policy:SSN-P04,Rev.2.1 , dated 1/12018) - Logical system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018	OK
A5.34	Privacy and protection of personal identifiable information (PII)	1	OK
A5.35	Independent review of information security	This is done through auditing plan mentioned before in clause (9.2 audit)and governed by the other procedures of control such as (Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018)	OK
A5.36	Compliance with policies, rules and standards for information security	It is stated by the head of operations and security that the operation team in coordination with QA dept as applying an audit plan (shown before) and check the results and compliance with ISMS policies and procedures	OK
A5.24	Information security incident management planning and preparation	Service reports are used as evidence in cases show the effectiveness of the concerned dept for response and resolution such as SFC (is an AOT customer) monthly report (SD-F03 May -2023)	OK
A5.19	Information security in supplier relationships	Through SLA agreement such as shown in GO SLA previously ((GO) with its SLA (Rev -2015) in the same standard clause (4.2 context of organization)	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.20	Addressing information security within supplier agreements	Through SLA agreement such as shown in GO SLA previously ((GO) with its SLA (Rev -2015) in the same standard clause (4.2 context of organization)	OK
A5.21	Managing information security in the information and communication technology (ICT) supply chain	Through SLA agreement such as shown in GO SLA previously ((GO) with its SLA (Rev -2015) in the same standard clause (4.2 context of organization)	OK
A5.22	Monitoring, review and change management of supplier services	Suppliers: are covered through SLA agreements, example such as communication links service provider (GO) with its SLA (Rev -2015) which is providing communication service to AOT Customer (Murabha)..this is reflected in service report(SD-F03, June,2023) with incident ID: I-009751 (Murabaha GO IP VPN link is down) and it is closed ref to GO feedback (mentioned in detail in the report clause 2.1 incident log) and shows the utilization measurements	OK
A8.32	Change management	Reviewed from the documents: - CO-P01 Configuration Management Procedure rev.10 dated 1/1/2018 - CO-P02 Change Management Process rev 1.0 dated 1/1/2018	OK
A8.4	Access to source code	(Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018) clause: 2.6 Software and Application Security	OK
A8.18	Use of privileged utility programs	Stated and shown in : (Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018) clause : 2.6 Software and Application Security	OK
A8.3	Information access restriction	Shown in file : (Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018) Clause : 2.1 Security Management and Control	OK

Clause No.	Requirement\\Departement	Evidence	Result
A7.10	Storage media	As an example (Physical Security and physical Access Control Policy:SSN-P04,Rev.2.1 , dated 1/12018)(Clause 7.3 :Secure area policy and equipments &Clause 7.3.1: :Physical media containing sensitive information) Reviewed through document (SSN-F02 Media Destruction Log, Rev 1.0, dated 1/3/2010) it shows the disposal committee member list and media type with all required signature for access and approval reviewed from document (Physical Security and physical Access Control Policy:SSN-P04,Rev.2.1 , dated 1/12018)	OK
A7.9	Security of assets off-premises	Shown in document : SSN-P03 Physical Security and Access Control Policy updated v1(rev 2.1 dated 1/1/2018) (clause 7.3:Secure Area Policy, sub clause 7.3.5 for portable devices)	OK
A8.2	Privileged access rights	All user access management is governed by users physical and logical policies the 2 files: -Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018 -Logical system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018 identify all AOT users access management	OK

Clause No.	Requirement\\Departement	Evidence	Result
A8.5	Secure authentication	It is reviewed with OP manager (Mr. Mohamed Abdel Rahman) and he stated that this is governed through physical and logical policies mentioned before PLUS the instructed rules file (Information Security controls & objectives:SSN-S02, Rev2.1, dated 1/1/2018) which has controls and objectives such as: -2.1 Security Management and Control -2.2 Security of Staff Members, Contractors and Agents -2.3 Network Protection -2.4 System Level Security	OK
A8.1	User end point devices	Shown within service report (SD-F03: Monthly Service report, dated May,2023 for AOT's customer SFC) It shows service provided , assets supporting services and ownership within security team leader (Mr. Alaa Helala) All user access management is governed by users physical and logical policies the 2 files: -Physical Security and physical access Control Policy:SSN-P04,Rev.2.1 , dated 1/1/2018 -Logical system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018 identify all AOT users access management	OK
A8.34	Protection of information systems during audit testing	It is shown within document :QM-F01 Audit Program, dated 1/5/2023, the time table within a full year 2023 and the 2nd one done on May , 2024 covering only 2 depts. Data center and CMDB	OK

Clause No.	Requirement\\Departement	Evidence	Result
A8.33	Test information	It is shown through process of development document : - SD-P03 Design And Transition Of New Or Changed Services Process , rev1.0 , dated 1/1/12018 - RS-F01 Release Management & release acceptance Plan-Initial revision , rev 1.0 , dated 1/1/2018	OK
A8.25	Secure development life cycle	Based in Egypt office and all departments are controlled through physical access control and logical access control as shown within audit and checked from the documents evidence such as : - (Physical Security and physical Access Control Policy:SSN-P04,Rev.2.1 , dated 1/12018) - Logical system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018	OK
A8.28	Secure coding	Shown in : Information Security controls & objectives document clause:2.6.2 Software design and development	OK
A8.26	Application security requirements	Shown within policy file of :Information Security Management System Policy, SSN-P27, rev2.1 dated 30.04.2023	OK
A8.16	Monitoring activities	Done by the control of the quality control manager(Mr. Sherif, Egypt office) with all needed tests to avoid any impact to customer side	OK
A8.9	Configuration management	Under change and configuration management policy an procedures Reviewed from the documents: - CO-P01 Configuration Management Procedure rev.10 dated 1/1/2018 - CO-P02 Change Management Process rev 1.0 dated 1/1/2018	OK

Clause No.	Requirement\\Departement	Evidence	Result
A8.12	Data leakage prevention	Shown within more than one evidence : - Information Security Management System Policy, SSN-P27, rev2.1 dated 30.04.2023 - SSN – 02: Networks and communications security policy, rev 2.1 , dated 1/1/2018	OK
A8.10	Information deletion	check policy for deletion of information defined in SSN-P27 Information Security Management System Policy documents (Revision No. : 2.1 | Revision Date: 30/4/2023)	OK
A8.11	Data masking	check Client SLA for data masking required and check data masking and encryption policy applied to client data	OK
A8.23	Web filtering	check firewall Fortigate policy for website filtering	OK
A7.4	Physical security monitoring	Check CCTV surivaillance cameras check exmple Cam #7 for Data Center outdoor and Cam #12 & Cam #14 inside Datacenter , and check CCTV logs	OK
A7.7	Clear desk and clear screen	Check Clear desk and Clear Screen in SSN-P27 Information Security Management System Policy documents (Revision No. : 2.1 | Revision Date: 30/4/2023)	OK
A6.8	Information security event reporting	Check incidient investigation reporting system in ITOP application ticketing system (Ticket # i-455642	OK
A5.7	Threat intelligence	check blocked IPs analized by Operation departments which defined as Threats due to unusal beheviuor such as many trials for entering username and password for client services	OK

Clause No.	Requirement\\Departement	Evidence	Result
A5.16	Identity management	Stated and Shown in file : -Logical system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018 Clause: 7.2. Logical Access Procedures Stated and Shown in file : -Logical in system access policy & procedures: SSN-P19, Rev2.1, dated1/1/2018	OK
A5.23	Information security for use of cloud services	Check Cloud security policy and certifcate for ISO 27017:2015 for AOT cloud used	OK

Strength Point

Availablity of resources and High Avaibility systems
Top Managment Commitment
Involvement of people

Area for Improvement

Need to elobrate more in business risk senarios and to consider in risk analysis asset paths and business processes and Desiert End State DES , As AOT work with governamental Sectors which could have Hacking to Governmental Business proceeses.

Observation

na

Minor NCR

na

Major NCR

na

Team Leader Recommendations

Recommed for Certifcation

Disclaimer Statement

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

Lead Auditor Name:
Adel Belal (AB) Signature