NSF-International Strategic Registrations

ASSESSMENT REPORT

Company Name and Location:	T.C. OKAN ÜNİVERSİTESİ	
Facility Type:	Site	
Customer # (FRS) / Job No.	C0176543/ J1332527	
Audit Dates (start/end):	30.12.2017&02-06 January 2018	
Total Audit Duration (days per standard):**	**ISO 27001:2013**	5.5 mandays
	Select standard	Click here to enter days.
	Select standard	Click here to enter days.
	Select standard	Click here to enter days.
	Select standard	Click here to enter days.
	Select standard	Click here to enter days.
	Select standard	Click here to enter days.
Report Date:	06 January 2018	

AUDIT TYPE & RECOMMENDATION*

Based on the customer performance trends, customer special status, suspension history, customer audit results (as applicable), repetition of major issues, nature of major issues, overall quality management system implementation and effective implementation of 100% resolved and closed NCRs, the audit team have made the following recommendation to NSF-ISR's certification decision authority:
(TS/IATF Only-Note: If any criteria from AESOP 3862, section 9.18 is met and withdrawal is not recommended, then the Lead Auditor must complete the justification below)
Justification for not recommending certification withdrawal:
Click here to enter text.

Surv. Audit: Continue Certification, NO CAR

**Recommendations/Results for RSL audits will affect related sites*
*** For TS/IATF Audits: Only report the number of days for the audit, excluding time spent on previous CAR verification or on-site audit planning.*

-Confidential-

CONTENTS
CUSTOMER REPORT SECTION

COMPANY AND AUDIT INFORMATION

Audited Company Address: Akfırat - Tuzla İstanbul Turkey

IATF Number of Audited Site (TS/IATF, if applicable): N/A

Company Management Representative (Name/Title): Mr. Emre Demirok

Audit Team Information:

	Name	IATF Cert. Number	Days/auditor**
Lead Auditor:	Özgün Okumuş	N/A	5.5 days
Team Auditor:	Click here to enter text.	Click here to enter text.	Click here to enter text.
Team Auditor:	Click here to enter text.	Click here to enter text.	Click here to enter text.
Team Auditor:	Click here to enter text.	Click here to enter text.	Click here to enter text.
Team Auditor:	Click here to enter text.	Click here to enter text.	Click here to enter text.
Team Auditor:	Click here to enter text.	Click here to enter text.	Click here to enter text.

Time added for past NC verification (not to be included above): N/A

Technical Expert(s): None

Observers: --

Internal Witness Auditor: --, Click here to enter text.

Objectives for this Audit: To determine maintain of certificate

Audit Scope: (See Company Certificate, Facility Record Sheet (FRS), or equivalent document / process)

To determine recertification of certificate

*** For TS/IATF Audits: Only report the number of days for the audit, excluding time spent on previous CAR verification or on-site audit planning. Identify TS/IATF audit time separately by indicating (TS) next to the reported days (e.g. 3.5 (TS)).*

AUDIT RESULTS

AUDIT SUMMARY

T.C. Okan University is a university which gives high education in several disciplines. Such as; Engineering, Management. They have nearly 498 employees which are generally professors and doctors. Internal audits were performed effectively. ISMS was established on manual, statement of applicability, procedures, policies and plans. ISMS was established on manual, statement of applicability, procedures, policies and plans and has been implemented over one year effectively. ISMS MR was new appointed at last year period. Internal audits were conducted as identified. Risk analysis plan was updated and republished. No incident has been occurred at last year period. Corrective actions were implemented after incidents, internal audits and security assessment findings, performance monitoring results. No nonconformity was found, four opportunities for improvement were determined as audit finding during this audit period. No nonconformity was determined during this audit period, two opportunities for improvement were determined as audit finding.

Maintain to certification on ISO 27001:2013 is recommended.

EXCLUSIONS or NOT APPLICABLE

The company has excluded the following requirements of the audit standard. The justification for the exclusions is noted below and is considered acceptable.

Annex A.10

DETAILS OF AUDIT FINDINGS

AUDIT FINDINGS

This audit identified # Major Nonconformities, # Minor Nonconformities and # Opportunities for Improvement (OFIs).

Details of the opportunities for improvement and any nonconformities are provided below.

CORRECTIVE ACTION REQUESTS (CARs)

None

NOTE: All corrective actions plans should be submitted within 30 days with corrective action implemented within 60 days. Major nonconformities must be verified by NSF within 90 days and minor nonconformities will be verified by NSF for effectiveness during the next audit.

OPPORTUNITIES FOR IMPROVEMENT (OFIs)

Note: OFI's are generally prefaced with the term "consider" and are documented in situations where the company does meet the requirements of the standard and may obtain some advantage by way of improvements in effectiveness or efficiency by considering the comments noted.

OFI No. 1: Archive area fire protection system can be improved
OFI No. 2: Entrance security area switch box protection system can be more effective

VERIFICATION OF PREVIOUS AUDIT CARS

There were no previous CARs recorded during the previous audit.

AUDIT DETAILS - PROCESSES / ACTIVITIES ASSESSED

PROCESS NAME: Security Assessment

PROCESS OBJECTIVES: Once a year assessment

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok (IS Management Representative- appointed on 22.10.2014), Şaban Budakoğlu assigned as ISMS Team Leader are process owners. Process is effectively implemented.

NOTES: ISO 27001:2013 clause 9 with Annex A.18

Measurement methods and control in risk procedure; risk definition and evaluation, definition of system controls and measurements are defined. Equipment to test list is identified on Form LS.BİS.007. System test reports were examined and approved. Network Vulnerability tests have done for three different systems. These systems are DMZ, Student Network, Servers and BİM Networks.

They have planned to done Vulnerability tests once in a year. This is subjected in Measurement and Control Procedure (PR. BİS.010). McAfee program to control vulnerability on Web sites, firewall and wireless and Karpersky is used for clients /users. The program could make several attacks to web sites. This program usage rights are owned by the T.C. Okan University. They are planning to make this tests once in a year and this is

subjected in Measurement and Control Procedure (PR. BİS.010). Last penetration test was performed on 16 March 2017 over IT system of university with BBS (Bilgi Birikim Sistemleri), no vulnerability was detected during this test period by using Netsparker program.

Other weaknesses are controlled by test program Netsparker. By means of this test activity, web implement security weakness, weakness scan, explosion test are performed. Last test was performed on 16 March 2017 by ISMS Team leader, no critical weakness was detected during this test period, no action required.

PROCESS NAME: Legal compliance

PROCESS OBJECTIVES: % 100 compliance to regulations

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

EmreDemirok is Process Owner. Legal compliance is detailed in manual BGYSEK 01 July 2015, rev.01.

NOTES: Annex A.18

Compliance with legal requirements are identified. Compliance with security policies and standards, and technical compliance are reviewed by IT manager periodically. National regulation for facilitating customs operations (nr 28524 - 10 January 2013) is regulated customs operations.

Personal data protection law, nr 6698, 24/3/2016

National Regulation for Internet publications (Regulation number 5651, 23 May 2007).

National regulation for Cyber Incidents Response Team (Regulation Nr: 28816, 11 November 2013) is started for implementation, team is generated.

PROCESS NAME: Contingency planning

PROCESS OBJECTIVES: % 100 compliance to regulations

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok is Process Owner. Process is effectively implemented. Business continuity plan – PL.BİS.002 is available.

NOTES: Annex A.17

Business Continuity plan PL.BİS.002, rev. 01, 19.11.2014 includes Including information security in the business continuity management process and business continuity and risk assessment and addresses information security requirements and identifies priorities for testing and maintenance. Plan documents rehabilitation of ISMS management system when unintended situation happens.

Business continuity and emergency practice plan Fr.BİS.014 was checked as:

Disaster Recovery emergency practice, 01.12.2017, managed by ISMS – MR

No action was requested (required) after this practice.

PROCESS NAME: Document Control

PROCESS OBJECTIVES: % 100 revision control

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Ms Banu Bayrak is responsible of process. Control of Document and Data Procedure - PR.KYS.001 is maintained.

NOTES: Clause 7.5

ISMS manual includes ISO 27001:2005 requirements and approved by General Manager. General elements are defined with implementations and procedure references. Some revision in procedures and no revision in other documents at last year period

Document Control procedure PR.KYS.001, rev.07, 31 May 2017 is used. Document master list is used to trace the distribution. Procedures, instructions and plan lists are used to trace revision status of the documents. Revision in documentation at last (procedure, instruction checked). Two procedures revised at last year period:

Samples

ISMS Manual (BGYSEK 01 July 2015, rev.01)

Malicious Software procedure PR.BİS.007, rev.01, 31 May 2017

Network and system management procedure, PR.BİS.001, rev.05, 31 May 2017

External documents are listed and controlled. Samples:

ISO 27001:2013 Standard

National Regulation number 5651 for Internet publications

National regulation for electronic communication security number – June 2008 were checked.

PROCESS NAME: Record Control

PROCESS OBJECTIVES: % 100 compliance to retention times

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Ms Banu Bayrak is responsible of process. Control of Document and Data Procedure - PR.KYS.001 is maintained.

NOTES: Clause 7.5

Quality records control procedure is used to regulate the record management. Record list is used to define responsibilities, retention time of the records. Electronic documents control and backup system is identified in relevant procedure as well. Archive record list is used. No revision in records at last period. Retention times sample:

Asset inventory list LS.BİS.002 retention time 1 year in department and 5 years at archive.

IS test tools list inventory list LS.BİS.002 retention time 1 year in department and 5 years at archive.

PROCESS NAME: Asset Management

PROCESS OBJECTIVES: % 100 compliance to regulations

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

ISMS Team is Process Owner. Process is effectively implemented. They are assessing the assets and risk during

the ISMS review meetings. Asset and Risk management procedure PR.BİS.011 rev. 00 -03.06.2013(Risk assessment Procedure) and Pr.Bİs.012-03.06.2013-Rev.00 (Asset Management Procedure) is documented and implemented for asset management and Risk Management. In this procedures determination of asset needs, determination of assets, determination of asset levels are identified. Asset and Risk management procedure PR.BİS.011 rev. 00 -03.06.2013(Risk assessment Procedure) and Pr.Bİs.012-03.06.2013-Rev.00(Asset Management Procedure) is documented and implemented for risk management and asset management.

NOTES: Clause 6&8, Annex A.8

Risk management plan documents asset identification, confidentiality level, information evaluation, threats, risk caused by this threats, impact of this risk to business, risk level, reaction for this risk, control of risk, calculation of reduced risk level, decision of control of acceptance and statement of applicability, responsible, date.

Information categories plan (LS.BİS.003) is documented for categorization of information. They have 11 categories (Such as, Storage Devices, Database etc..) and 5 confidentially categories (such as top secret, secret, personal etc).

Asset codes, identification, group, status, location, ownership and value are recorded and followed up in the Asset Inventory List (LS.BİS.002). 102 asset group were identified.

Samples

Asset Name: Web server

Asset Category: virtual server

Responsible : IT

Confidentially Category: Secret

Asset Name: academician database (OLB)

Asset Category: virtual server

Responsible: IT

Confidentially Category: secret

PR.BİS.011 rev. 00 -03.06.2013(Risk assessment Procedure) is documented and implemented for risk management. Methodology of risk management is identified in this procedure as:

Risk point = Information evaluation with hazard impact x Possibility x Noticeability

Company has been established and implemented risk management system for ISMS. This risk management system includes definition of risk assessment approach, risk identification, analysis and evaluate the risks,identify and evaluate options for the treatment of risks ,select control objectives and controls for the treatment of risks, Obtain evidence of management authorization to implement and operate the ISMS, review the Statement of Applicability. Risk level classification methodology is identified as below:

All assets will define according to asset Management Procedure PR.BİS.012, For each asset weaknesses should be defined. All weaknesses will be listed on LS.BİS.004/rev.00 and risk will be defined according to weaknesses

lists.

After completion of risk identification, Risk assessment should be done on each risk according to PR.BİS.011 Risk assessment Procedure.

Okan University is using a web based program (www.uygulamalar.okan.edu.tr/envanter) which is produced by IT department of Okan University for tracking assets.

Samples for risk plan;

Asset: OLB website

Weakness:

- wrong access permit

Threat:

- information leakage

Risk Evaluation:

Risk point = Information evaluation with hazard impact x Possibility x Noticeability

Risk Point(1) = 3x1x3=9

Asset Risk evaluation and management system is effectively established and implemented.

Action:

- Access rights Control Table is implemented

Risk category is classified as below

0-10 –acceptable Risk – No Action nor Control Needed, 10-40 medium risk –Action and control required, 40-50 – high risk– action required

PROCESS NAME: Statement of applicability

PROCESS OBJECTIVES: % 100 compliance to control objectives

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok (Leader of ISMS) is Process Owner. Process is effectively implemented. Statement of applicability LS.BİS.010 approved by ISMS MR and republished during transition to ISO 27001:2013 standard

NOTES: ISO 27001:2013 Clause 6.1.3

Statement of applicability includes:

- National regulations
- Contract requirements
- Business requirements
- Risk analysis result

In statement of applicability(Form LS.BİS.010/Rev01 /11 MAY 2015) realization of selected controls are identified

according to Annex A of ISO 27001:2013 standard (all clauses of this Annex are addressed with selected controls).

PROCESS NAME: Internal Audits

PROCESS OBJECTIVES: At least twice a year

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok (ISMS MR) is Process Owner. Process is effectively implemented. Internal audits procedure PR.ICD.001 is documented and implemented for ISMS.

NOTES: ISO 27001:2013 Clause 9.2

Internal audits procedure PR.ICD.001 is documented and implemented for ISMS. Internal audits are conducted at least once a year.

Internal audit plan PL.ICD.001 which shows ISO 27001 elements and auditors is documented and checked for year 2014.

Internal auditors are trained for ISO 27001 standards and independent from audited department. Trained internal auditors are:

- Emre Demirok (Leader of ISMS Team)

- Şabna Budakoğlu(Member of ISMS Team),

- Samir Çakır IT Support Expert

- İzzet Özen(Member of ISMS Team),

- Alper Burul (Member of ISMS Team)

- Semra Coşkun (Member of ISMS Team)

- Banu Bayrak (Member of ISMS Team)

- Gamze Güçkıran(Member of ISMS Team)

All ISO 27001 clauses and items were audited during last audit period. Internal audit form RP.ICD.001 is used for reporting of internal audits.

Internal audit questionnaire LS.İCD.001 is used for check-list of audit and prepared item of standard basis and includes Annex A requirements of standard.

Last internal audit was conducted on 08 November 2016. Last internal audit cycle covers all processes & organizational functions. 2 minor nonconformities were determined during this audit period.

Sampled as;

- System room access monitoring device was not effective
- Obsolete revision Termination of contract form (FR.İNK.009) is used

PROCESS NAME: Improvement

PROCESS OBJECTIVES: % 100 compliance to action due date

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok (ISMS MR) is Process Owner. Process is effectively implemented. Corrective and Preventive Actions Procedure PR.KYS.003 is documented.

NOTES: ISO 27001:2013 Clause 10 with Annex A.16

Actions implemented after internal & external audit non-conformances, incidents etc. are recorded to "Corrective and Preventive Actions Demand Form FR.KYS.001. Due date, relevant departments, actions and results are seen in this form.

Corrective and preventive actions are followed by "Corrective and Preventive Actions Table". NC's are followed with CA are classified as from internal and others from risk analysis audit, incidents.

This form includes the root-cause analysis and effectiveness evaluation of the corrective and preventive actions. Information security events shall be reported to ISMS Team Leader by means of Incident Report. ISMS Team Leader monitors incidents and related actions as well. Corrective and preventive action is initiated when an incident occurs according to corrective and preventive action procedure.

Corrective and preventive actions are followed by "Corrective and Preventive Actions Table".

2 corrective actions were initiated and closed after internal audit

sampled as;

- System room access monitoring device was implemented
- New revision Termination of contract form (FR.İNK.009) was distributed and used

<u>Information security incident management:</u>

Incident reporting procedure PR.02 documents management of ISMS incidents. This procedure includes:

- Reporting information security events
- Reporting security weaknesses
- Responsibilities and procedures
- Learning from information security incidents
- Collection of evidence

Information security events shall be reported to ISMS Team Leader by means of Incident Report FR.BİS.001. Weaknesses of management system is identified in Asset Management system and in this method: all employees, contractors and of information systems and services note and report any observed or suspected security weaknesses in systems or services to ISMS Team Leader periodically. ISMS Team Leader monitors incidents and related actions as well. Corrective and preventive action is initiated when an incident occurs according to corrective and preventive action procedure.

No incident has been occurred at last year period.

PROCESS NAME: Management Review

PROCESS OBJECTIVES: Review meeting at least once a year

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok (ISMS MR) is Process Owner. Process is effectively implemented. Management review is documented and implemented as mentioned in ISMS manual. This procedure includes frequency and agenda of management review meetings. Interval of management review meeting is at least once a year. By means of this management review meeting continual improvement of ISMS process is identified.

NOTES: ISO 27001:2013 Clause 5 with Annex A.5

Management review procedure is documented and implemented. This procedure includes frequency and agenda of management review meetings. Interval of management review meeting is at least once a year.

Management review meeting form FR.OKN.001 is used for reporting of results and decisions of management review meeting.

Last management review meeting was held on 04 December 2017

Agenda

Previous meeting evaluation

Audit results

Feedback from interested parties

Corrective preventive actions

Risk analysis results

ISMS coordination and risk board meeting results

ISMS Effectiveness measurement

Technical compliance penetration test evaluations

ISMS Objective

ISMS Improvement techniques evaluation

Participants of meeting

Şule KUT, Rector of University

Güner Gürsoy, Assistant of Rector

Şaban Budakoğlu, ISMS Team Leader

Banu Bayrak, QM Expert

Emre Demirok, , ISMS MR

Mustafa tufan, IT Manager

Security policy

Company has been documented and maintained a security policy for the implemented ISMS. ISMS Policy document PO.BİS.001 and first published on June 03, 2013. At This policy is approved by General Manager and announced to all interested parties by means of electronic ways. In six months periodic review is performed by management on policy in order to verify effectiveness and sufficiency.

ISMS objectives are documented in objective monitoring form. These objectives are approved by General Manager of company. Realizations of these objectives are scheduled in this form with related responsible, resources, actions, due dates and results of actions. Follow up system of ISMS objectives realizations are effective.

Samples for 2017

- Number of security test defect 0
- Training given to per staff 5 h
- Number of IS incident 0
- Compliance to national regulations % 100
- Business continuity practices 1
- Number of information leak event 0
- Number of system break down 0
- Number of unauthorized access 0
- Discipline process implement 0

PROCESS NAME: Training

PROCESS OBJECTIVES: % 100 Compliance to training plan

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Mrs Seren Kumrulukuş is responsible for HR and Training activities. Employee Security Policy PO.BİS.003 is documented and implemented.

NOTES: ISO 27001:2013 Clause 7 with Annex A.6 & A.7

Staff competencies are documented in Job descriptions as education, training, experience and skills separately.

Staff individual files based on national labor law (4857).

- Müge yavaş, instructor (asst. prof.), recruitment: 01.03.2017, work experience: 2 years, graduation: dentist department of university

Training participant form Fr.INK.015 /Rev.00, Training Plan PL.INK.001/Rev.00, sample trainings

- ISO 27001:2013 General Training, on 20.11.2017, Trainer: Enderun consultancy, number of participants: 27
- ISMS acknowledgement training, on 04.12.2017, Trainer: Enderun consultancy, number of participants: 15

Orientation training is given to new hired staff;

Tuğçe İskender, 04.12.2017, training center expert

Gizem gazez, 02.11.2017, HR expert

Organization of information security

Responsibility and authority is described as job descriptions in department Personnel roles and responsibilities document no. OEK Rev 02 and organization chart ŞM.İNK.001 rev. 08 is available in this document.

Sample job descriptions:

- ISMS Team Leader job description – GT-INK.020/rev.02
- HR Department responsible job descriptions – GT-INK.091, rev. 01

Mr. Emre Demirok who is business administration graduation and 15 years work experience in IT department is new appointed on 14.03.2016 as ISMS Management Representative, assignment letter was checked.

Information Security Management System Team Leader Mr. Şaban Budakoğlu who is business administration graduation and 11 years work experience in IT department – appointment letter 14.03.2016.

ISMS Team appointment letter 14.03.2016 dated, approved by University Rector.

Company staff and third party personnel who can access IT system sign confidentiality agreement in order to ensure information security. At the same time, risks for external access and process to assets are identified. Sample confidentiality contracts were checked.

Human resources security:

Roles and responsibilities for security of staff are identified in job descriptions. All employees and subcontractor staff sign agreement while recruiting; this agreement includes related national regulations, discipline process when they damage information security, during resignation/abolishing of contract handing back of possessed assets, cancelling of access rights. Sample contracts were checked on form FR.İKN.007.
Screening - background verification checks on all candidates' crypto- clearance by policy.
Regular trainings and updated are given to all employees, contracts are signed with staff and subcontractor for information confidentiality.

Sample contracts checked for confidentiality;

Neslihan çınar, HR department responsible, date of contract: 01.12.2016

Samples for termination of contract

Nilay Utlu, academic personnel, date of termination 15 November 2017

Seren Kumrulukuş, HR personnel, date of termination 30 November 2017

PROCESS NAME: Supplier Relations (includes Physical Security)

PROCESS OBJECTIVES: % 100 Compliance to specification and maintenance plan

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Purchasing Department is the Process Owner. Process is effectively implemented. Operation control procedure PR.BİS.006 is documented and implemented.

NOTES: ISO 27001:2013 Clause 7 with Annex A.15 & A.11

Resource needs are clearly defined according to "General Resource Management statement" to improve satisfaction of customers and reviewed in management reviews. Resources are allocated effectively and satisfactorily by management documented in corporate budget plan as well. Project budget and analyses form is used for monitoring of required finance and results.

Supplier relations:

Date of order: 07.09.2017

Device: laptop

Supplier: BBS bilgi birikim sistemleri

Code: Lenovo e-570

Quantity: 1 unit

Date of incoming: 07.09.2017

Invoice: BB2017000003937

Supplier Evaluation: % 95

Supplier confidentiality contract are signed and kept by purchasing responsible, if required SLA requirements are documented in contract, sample confidentiality contract is checked for

Fornet bilgisayar sistemleri co, ERP solutions supplier specially accounting and HR activities, date confidentiality contract 07.01.2015 (continuing)

Physical and environmental security:

Cameras, secure area, server, network switches, office devices, cables, power supply, special designed building for natural disasters (earthquake etc.), Network switches (WIFI, router, switch equipment). All secure places is limited access based on authorization.

Only authorized personnel can enter the controlled areas.

Cameras can monitoring by authorized employees and locked doors are secured by PRONET which is a security Company. After entering a room, a pass code need to enter in 10 second otherwise an alert activated. If they enter a pass code than a SMS will send to responsible person to inform.

Mobile phones and video and audio recorders are allowed. Temperatures of the server rooms are controlled and high temperature alarm is available. After 20 C degrees, air conditioners starts to work and try to decrease room temperature under 20 C degrees. Higher floors and water leakage detectors are also available.

Higher floors, sensors, fire detectors and extinguishing systems are available.

Physical and environmental security procedure PR.BİS.005 is documented and implemented for physical and environmental security of equipment. This instruction considered to reduce equipment risks caused by environmental and other threats such electricity cut-off. Besides instruction includes protection management of data, IT support electrical and communication cables. Periodic maintenance system is implemented for equipment.

Daily, weekly, monthly, three months, six months and annual maintenance is planned and performed according to instruction above. PR.BİS.002

Each Devices has a unique control form.

UPS, 06.11.2017, maintenance by inform electronic co, report nr 641538

Sever room air-conditioning, 12.12.2017, by Erkan Ağaç system support expert

Alarm system12.12.2017, by Erkan Ağaç system support expert

Network distribution cabins, 24.08.2017, by Ayhan YILMAZ system support expert

Engineering laboratory user computers, periodic maintenance, 21.07.2017, by Alper BURUL system support experts

Air-conditioning, 16.03.2017, maintenance by Güngör Klima

Access turnstile at entrance of university, 01.11.2017, by Selçuk Çiftçi

Fire alarm detector at secure areas, 09.05.2017, by pronet co

Fire tubes, last inspection for secure areas on 12.06.2015, form nr SSS-FR-04, performed by Kalafatoğlu Yangin Ekipmanlari Fire Co.

PROCESS NAME: IT Operation

PROCESS OBJECTIVES: % 100 Achievement of control objectives

CUSTOMER SPECIFIC REQUIREMENTS, IF APPLICABLE (Mark this as NA for any EH&S Audits): N/A

Emre Demirok (ISMS MR) is Process Owner. Process is effectively implemented.

NOTES: ISO 27001:2013 Clause 8 with Annex A.9 &A.10&A.12&A.13&A.14

Company has been established, documented, implemented and maintained according to Measurement methods and control in risk procedure (PR. BİS.010) in order to monitoring and review of ISMS.

Company has periodically review effectiveness of ISMS by means of paying attention to security audit results, breach incidents, effectiveness measurements, suggestions and feedbacks of related parties. This review

includes whether security controls meet requirements.

Company has established and implemented a system in order to verify effectiveness of measurement controls whether meet security requirements.

Measurement methods and control in risk procedure (PR. BİS.010); risk definition and evaluation, definition of system controls and measurements are defined. This procedure identifies methods for instantly determination of errors after processing, security breakings and breach incidents, effectiveness of security activities which delegated to staff by management, prevention of security breach incidents, making decision for effectiveness of preventions in order to solve security breakings. Equipment to test list is identified. System test reports were examined and approved by BBS (Bilgi Birikim Sistemleri) Team leader. Last test report was checked as exposure level is used for system tests on 16 March 2017 by using Netsparker Program. Network Vulnerability tests have done for four different networks. These networks are DMZ, Student Network, Serversand BİM Networks. They have planned to done Vulnerability tests once in a year. This is subjected in Measurement and Control Procedure (PR. BİS.010). They are using a Acunetix program to control vulnerability on Web sites. The program could make several attacks to web sites. This program usage rights are owned by the T.C. Okan University. They are planning to make this tests once in a year and this is subjected in Measurement and Control Procedure (PR. BİS.010). Unofficially this program could usable according to users desire and differences on web pages. Like new interface.

Test Devices List Ls.BİS.007/rev.00 is using to tracking test they had before.

Communications and operations management

Against virus, the security program Kaspersky is installed for all desktops and updated periodically. Against Firewall and spyware threats, security is maintained. The limitation of internet usage is not implemented for each computer (firewall –URL blocking).But they are monitoring each user by limiting internet usage by a security interface.

Karsperski log: virus 1-okn 27.11.2017, quarantined and deleted.

With Fire wall: access control, MAC filter, URL blocking, schedule rule: time limitation, intrusion detection: SPI and anti dos detection, RIP defect, over DMZ. NAT Address Mapping and Mapping table usage, it is monitored who wants to access where

Daily, Weekly and monthly offline backup system is conducted on DVD media. Back up instruction is documented and implemented, daily SQL back up is performed. Symantec Backup Exec 20120 R3 software is using for backup. Back up Procedure PR.BİS.014 is using properly.

Access control

Active Directory is used for monitoring of access control. TOOLS configuration management. Firmware, DeepFreeze program to back to first situation defaults, STATUS: IP reports. User responsibilities are documented and explained in staff User Identification/ Authorization and agreement form FR.INK.007 rev.01.

Wlan sytem is using for arranging 4 different servers. Like Student and Okan. Each user permissions could control by IT. Each user in the University need to defined by IT and sign in while they are using the internet.

Access controls are available, over this line defined e-mail ports or any ports can be blocked and alternative ports can be identified or not allowed.

Log records are controlled and reported by IT management, sample log report

Date: 12.12.2017

Time: 12:06

Source IP: 10.50.1.23

Destination URL: www.phoenix.edu.tr

Error follow up form LS.BİS.11 checked, no error has been detected at last year period.

Back up system is checked and found adequate, backup 05.10.2016 – all artificial server and local server data was stored by Gamze güçkıran software dept. manager.

System Control form is used in order to reduce threats at risk plan, conducted by quarterly, last control was performed on 06.09.2016 by izzet özen system unit manager over system assets (including firewall, IPS, crypto log, switches, exchange server, student information system server, etc.).

Remote access control form FR.BİS.009, is used and checked for application of Mr Hakan Özkan (HR Manager) on 18.10.2015.

Local admin. Authority demand is checked for application of Mr. Güner Güry (Asst. Rector), on 06.12.2017, authority is approved.

PROGRAM SPECIFIC REQUIREMENTS

ISO 20000-1 and ISO 27001 SPECIFIC REQUIREMENTS

ISO 20000-1 and ISO 27001 Program Specific Requirements

1. For ISO 20000-1: Does the registration audit schedule include a sample of the Business Relationship and Supplier Relationship services or activities that interface with the ITSMS but are not completely within the management and control of the ITSMS (ex: outsourced services, satisfaction survey requirements, etc.).

   YES ☐
   NO ☐
   N/A ☒

   ANSWER: Click here to enter text.

2. For ISO 20000-1 Did you review the organization's ISMS system (reports) to ensure that it is capable of addressing pertinent security control objectives of all Regulatory Compliance laws that the organization is subject to, and the maintenance of those control objectives.

YES ☐
NO ☐
N/A ☒

ANSWER: Click here to enter text.

3. For ITMS, did you evaluate (provide comments as necessary):

a. Organizations evaluation of information security related risks and the resulting ISMS design.

YES ☒
NO ☐
N/A ☐

ANSWER: Risk Management Procedure PR.BİS.011 is implemented. Risk management plan FR.08.03 documents asset identification, confidentiality level, information evaluation, threats, risk caused by this threats, impact of this risk to business, risk level, reaction for this risk, control of risk, calculation of reduced risk level, decision of control of acceptance and statement of applicability

b. The organization procedures that identify the criteria for significant information security related threats to assets, vulnerabilities and impacts on the organization and that the information related an asset, a vulnerability or a threat is managed within the ITSMS.

YES ☒
NO ☐
N/A ☐

ANSWER: They have PR.BİS.007 Protection from malicious software Procedure and PR.BİS.010 Measurement and Control Procedure.

c. The organization demonstrated that the analysis of security related threats is relevant to the organization.

YES ☒
NO ☐
N/A ☐

ANSWER: Isms objectives are identified. Company using PL.BİS.001 Risk Plan for entering and tracking risks.

d. The Statement of Applicability.

YES ☒
NO ☐
N/A ☐

ANSWER: Statement of applicability MS.BİS.010 is applicability was reviewed and approved on 11.05.2015 rev. 01.

e. Derived objectives and targets.

YES ☒
NO ☐
N/A ☐

ANSWER: Number of security test defect 0, Training given to per staff 5 h, Number of IS incident , Compliance to national regulations % 100, Business continuity practices 1, Number of information leak event 0, Number of system break down 0, Number of unauthorized access 0, Discipline process implement 0

f. Performance measurement and reporting against these objectives.

YES ☒
NO ☐
N/A ☐

ANSWER: Measurement Method and Controls Procedure PR.BİS.010 is documented.

g. Security and management reviews.

YES ☒
NO ☐
N/A ☐

ANSWER: Management review procedure is documented and implemented. Management reviews are performed according to Management Review Procedure PR. OKN.001. Review records are taken to Meeting Minutes Form FR.OKN.001

h. Management responsibility for Information Security Policy

YES ☒
NO ☐
N/A ☐

ANSWER: Management reviews are performed according to Management Review Procedure PR. OKN.001. Review records are taken to Meeting Minutes Form FR.OKN.001.

i. Links between Policy, Security Risk assessments, Objectives & targets, responsibilities, programs, procedures, performance data, and security reviews.

YES ☒
NO ☐
N/A ☐

ANSWER: Linked in Statement of applicability LS.BİS.010.

j. Are there inconsistencies between the organization's policy, objectives and targets and its procedures.

YES ☐
NO ☒
N/A ☐

ANSWER: Click here to enter text.

k. Where the organization is subject to Regulatory Compliance, the organization is responsible for the maintenance and evaluation of legal compliance. The Auditor may obtain checks and samples to verify this capability and that the organization has taken action in cases of non-compliance, with their specific Regulatory requirement. This may be obtained, but not limited to, reviews, performance data gathering by the organization and specific Stage 1 corrective actions implemented as a result of such reviews.

YES ☒
NO ☐
N/A ☐

ANSWER: Information management system relevance regulations are listed on External Document List National regulation for electronic communication security, nr 26942- National regulation for internet publications , nr 5651.

4. Were detailed audit trails described in the audit note section of the audit report that included the records that were reviewed to demonstrate the audit of specific applicable controls obtained by way of the completed SOA and / or Appendix D completed from ISO 27006.

YES ☒
NO ☐
N/A ☐

ANSWER: Detailed in Statement of applicability LS.BİS.010.

5. Have all client exclusions been clearly justified including exclusions related to controls. It is important to include the records the audit team reviewed that support the exclusion (s).

YES ☒
NO ☐
N/A ☐

ANSWER: Annex A.10 is excluded, specific justification is identified in Statement of applicability LS.BİS.010 rev. 01.

APPENDIX

The information in this section shall not be included in the report left with the customer. You will need to attach this section of the report in IQ as a separate attachment. The Customer Report (Sections that include Executive Summary through Program Specific Requirements sections, as applicable) should be left with the customer and attached in IQ. NSF-ISR AP auditors should submit applicable sections of the report to the appropriate NSF-ISR Asia Pacific office staff member in the Suzhou office.

FRS Number (or equivalent document / process): C0176543

APPENDIX DOCUMENTS
FRS Changes (or equivalent document / process):
Opening Meeting
Closing Meeting
Auditor Self Assessment Checklist - THIS IS LOCATED AT THE END OF THE DOCUMENT AND MUST BE COMPLETED

TS/IATF 16949: VERIFYPLAN: SECTION 0. ON-SITE PRE-PLANNING VERIFICATION (1 HOUR MIN)

1) Immediately prior to the opening meeting, did you:
   a) Review online, current customer reports and/or scorecards?
   b) Verify changes to current customer and internal performance data?
   c) If there were changes to performance data, did you adjust the audit plan?

   Was the audit plan revised? If YES, please describe the change and the reason for the change:

   Click here to enter text.

2) PERFORMANCE (TS/IATF 16949) Please verify and summarize all current performance data (i.e. product quality, delivery and special status) for all automotive customers (please prioritize IATF OEMs). The summary should include each IATF OEM Supplier code and written info on the actions implemented when performance was not met. (NOTE: All Suppliers to Ford, FCA and GM shall have access to their customers' systems).

   Click here to enter text.

3) Was an NCR created against 5.2 because the client did not:

   a) Know how to interpret the customer scorecards
   b) Access the customer supplier portals; or,
   c) Provide required pre-planning information

   Click here to enter text.

FRS Changes (or equivalent document / process)

1. Has the company name and/or address changed (NOTE: VERIFY THAT THE COMPANY NAME/ADDRESS ON SCORECARDS, Purchase Order, Contracts, etc., MATCHES THE FRS/NSF-ISR certificate).

   Yes ☐

   No ☒

   If "Yes", Describe changes

Click here to enter text.

Has there been a change in total employees?

Please identify the new employee count by shift(s), including temporary/seasonal employees and contractors.

Answer: Choose "Yes" if there are changes. Choose "No" if there have been no changes

Yes ☐

No ☒

Complete the following table to indicate changes in employee count

SHIFT	HOURS	EMPLOYEE COUNT
1	Click here to enter text.	Click here to enter text.
2	Click here to enter text.	Click here to enter text.
3	Click here to enter text.	Click here to enter text.
4	Click here to enter text.	Click here to enter text.

2. **Did you verify that the supplier codes are accurately identified on the FRS? If not, please make corrections in this section of the report.**

Answer: Choose "Yes" if there are changes. Choose "No" if there are no changes.

Yes ☐
No ☒

If "No", please make corrections in this section of the report.

SUPPLIER	SUPPLIER CODE
GM (9 Digit DUNS number)	Click here to enter text.
Ford (5 characters, alphanumeric)	Click here to enter text.
FCA USA (formerly Chrysler) (5 digits which could be followed by 1 or 2 capital letters	Click here to enter text.
FCA Italy (formerly Fiat, XYYY, where X is a letter and YYY is the number	Click here to enter text.
Daimler (8 digits)	Click here to enter text.
PSA Peugeot Citroen (maximum length is of 10 positions with any characters)	Click here to enter text.
Renault	Click here to enter text.
BMW	Click here to enter text.
Volkswagen	Click here to enter text.

3. Have there been any changes to processes, product lines, facility locations, key management, ownership, etc. that may impact the client's scope of registration? If "Yes", please explain in the notes section.

Yes ☐
No ☒

If "Yes", Describe changes

Click here to enter text.

4. Has there been a change in the PO number

Answer: Choose "Yes" if there are changes. Choose "No" if there are no changes.

Yes ☐
No ☒

If "Yes", provide the new PO Number: Click here to enter text.

5. **Is the remote support location information on the FRS (see section "Sites that provide support to this location") correct?** Note: A Remote Support Location provides non-production support to the site, e.g., sales, design, purchasing, shipping, storage (warehouse), APQP, etc. This location does not do anything/change the parts shipped to customers.

YES ☐
NO ☒

If "Yes", then provide the address(es) and identify each process(s) the location provides (e.g., design, sales, etc.)

STREET ADDRESS	CITY, STATE, ZIP	SUPPORT PROVIDED
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.

6. **Based on the above question, are changes to the current certificate required? NOTE - if reassessment, customer will get new certificate upon cert decision approval**

Yes ☐
No ☒

If "Yes", Describe changes

Click here to enter text.

7. **Are any support function audited by a different CB?**
   TS/IATF ONLY
   YES ☐
   NO ☐
   If yes, please review and attach a copy of that audit report, audit plan that and Certificate for that remote function. NOTE: If there any remote support locations that are audited by a different CB, please review, and attach, a copy of the last audit report, audit plan, findings (closed), and other CB's certificate. It is important that there is evidence that the other CB audit documents relate to the support activities it provides to this site.?

   YES ☐
   NO ☐

8. **Does the client need assistance on how to access NSF Online?**
   YES ☐
   NO ☒
   If "YES" Please indicate the contact name and phone number of the person needing assistance

Click here to enter text.	Click here to enter text.

9. **What is the next scheduled audit date? If customer is due for a reassignment, please recommend an auditor.**

   YES ☒
   NO ☐
   If "YES" Please indicate the date(s) in the following table

AUDIT DATE(S)	AUDIT TYPE
December 2017	2nd Surveillance
Click here to enter text.	Click here to enter text.

Opening Meeting

1. **Opening Meeting Date:** 30.12.2017
   Note: Ensure date matches OASIS calendar
2. **Attendance:**
   Option: Attach Audit Attendance

Attendees: Emre Demirok, Banu Çelebi, Semra Coşkun, Hüseyin Akduman, Dilek Türkkan, Şaban Budakoğlu, Banu Bayrak, Serhat Kara

3. **Please Review Each Of The Following Opening Meeting Topics**
   a. Introduction – Discuss Role Of Each" Auditor
   b. Attendance Sheet Circulated (If Necessary)
   c. Confirm Escort/Guide
   d. Confirm Confidentiality/Nondisclosure Agreement
   e. Review Scope/Objectives Of Audit
   f. Discuss Audit Process: Sample Of Management System And Processed Based
   g. Review Audit Schedule (Revise As Needed)
   h. CARS – Auditor/Auditee Responsibilities
   i. Definition Of Major/Minor Non-Conformance/Opportunity For Improvement
   j. Appeals Process
   k. Daily Meetings
   l. Closing Meeting Time/Date/Place
   m. Review Site Safety/Emergency Procedures
   n. Identify And Clarify Communication Links
   o. Confirm Working Arrangements – Hrs./Lunch/Auditor Facilities

   Did you cover all the above items during the Opening Meeting?

   YES ☐

   NO ☐

4. **Use of NSF-ISR Mark**
   Describe how the organization advertises its certification. Explain how the organization uses NSF-ISR and/or Accreditation Body Marks. Cite specific examples. Confirm organizations use of marks and statements of certification are in accordance with NSF-ISR Policies for Accredited Registration Services. (Mark as N/A if not applicable).

Click here to enter text.

Closing Meeting

1. **Closing Meeting Date:** 06 January 2018

2. **Attendance:**
   Option: Attach Audit Attendance

   Attendees: : Emre Demirok, Banu Çelebi, Semra Coşkun, Hüseyin Akduman, Dilek Türkkan, Şaban Budakoğlu, Banu Bayrak, Serhat Kara

3. **Are the following closing meeting topics covered?**
   a. Stress Appreciation For Cooperation/Hospitality
   b. Attendance Sheet Circulated
   c. c. Customer Review And Approval Of FRS (or equivalent document / process)Including Scope Statement On The FRS (or Review With Client)
   d. State Purpose Of Meeting
   e. Recommendation Of Audit Team
   f. Management System Strengths/Features
   g. Management System Features To Be Improved.
   h. Audit Report Summary: Review Scope/Objective of Audit/Sampling of Management System; Definitions of Major/Minor Nonconformance; Audit Summary Sheet – Conformance to Audit Standard.
   i. Corrective Action Response (Cars) Request Process:
      1. Identify Immediate Problem
      2. Root Cause Analysis
      3. Prevention (Solicit Commitments And Timing Of Implementation)
      4. CARs Must Be APPROVED Within 60 Days of Today or Prior To Certificate Expiration (Whichever Comes First.
         a. Final Report – Process/Content/Timing
         b. Explain The Decertification Process as applicable to the current audit result (TS Rules, Section 8)
         c. Confidentiality
         d. Appeals Process
         e. Explain Verification Audit, If Applicable

   j. If Recommendation Is To Register:

1. Management System Changes, If Applicable
2. Registrar Changing Rules
3. Maintaining Customer Complaint Record
4. Surveillance Audits
5. Leave Draft report with the customer.

NOTE for TS/IATF: Please remind the client that the complete audit record for this visit will include the report file along with the completed attachment list as follows: Pre-planning form (AESOP 8203); Audit agenda (AESOP 13680); TS/IATF Matrix (AESOP 9207); and the latest FRS document.

Did you cover all the above items during the Closing Meeting?

YES ☐
NO ☐

ATTACHMENTS

The documents in this section shall NOT be included in the report that goes to the customer. They do need to be attached in IQ along with the Customer Report (Sections that include Executive Summary through Program Specific Requirements sections, as applicable) and the APPENDIX sections of this document. NSF-ISR AP auditors should submit applicable sections of the report to the appropriate NSF-ISR Asia Pacific office staff member in the Suzhou office.

ATTACHMENTS – Attach these documents in Oasis
AESOP 13045 Audit Summary Matrix for 9001 based standards (including 13485)
AESOP 13048 14001 Audit Summary Matrix
AESOP 13049 18001 Audit Summary Matrix
AESOP 13050 27001 Audit Summary Matrix
AESOP 13051 20000 Audit Summary Matrix
AESOP 11661 Audit Plan
AESOP 12613 AQMS Pre Planning form
AESOP 10132 Draft Report for TS/IATF 16949 Only –in lieu of the draft report, this Customer Report (Sections 1 through 8) can be left with the customer but it **MUST be emailed to tsauditreports@nsf-isr.org or faxed to 734-827-3836**. **3836 NSF-ISR Asia Pacific auditors should submit their reports to the appropriate NSF-ISR Asia**

Pacific staff member in the Suzhou office.
AESOP 9207 Audit Summary Matrix for TS/IATF 16949 only
AESOP 8203 Pre Planning Form for TS/IATF 16949 only
AESOP 13680 Audit Agenda Form for TS/IATF 16949 only

AUDITOR SELF ASSESSMENT CHECKLIST

THIS IS A REQUIRED DOCUMENT THAT MUST BE COMPLETED. IT IS NOT TO BE PARTY OF THE AUDIT REPORT OR SUBMITTED TO THE CUSTOMER

COMPLETE THE FOLLOWING TABLE:

	QUESTION	YES	NO	N/A
1	Is there an audit plan/schedule (11661) associated with the Stage 1 activity?	☐	☐	☒
2	Was the Stage 1 Audit Report submitted through the Oasis within 3 days from the closing meeting? **3836 NSF-ISR Asia Pacific auditors should submit their reports to the appropriate NSF-ISR Asia Pacific staff member in the Suzhou office.**	☐	☐	☒
3	Was an Audit Pre-planning Form (8203) completed appropriately and attached in OASIS? NSF-ISR Asia Pacific auditors should submit the pre-planning form to the appropriate staff member in the Suzhou, China office.	☒	☐	☐
4	If Audit Pre-Planning (8203) was done on-site, was additional time added to the audit, PRIOR to the opening meeting and included on the schedule? NOT ALLOWED FOR STAGE 2 AUDITS. **TS/IATF ONLY**	☐	☐	☒
5	Was the pre-planning information used to analyze how it impacts the audit plan?	☒	☐	☐
6	Was the audit plan adjusted based on pre-planning and documented in the Audit Report?	☒	☐	☐
7	If any remote support location is audited by another IATF recognized CB, then have you uploaded all required records listed in TS Rules, 5.5, Option 2 (page 22)? **TS/IATF ONLY**	☐	☐	☒
8	Are all published Audit Plans attached in OASIS/iAudit ?	☒	☐	☐

	NSF-ISR Asia Pacific auditors should submit the audit plan to the appropriate staff member in the Suzhou, China office.			
9	Was the Audit Plan/Schedule created using the client's process names? If not, then revise.	☒	☐	☐
10	Does the audit plan support 8 hour audit day minus lunch times?	☒	☐	☐
11	Were the appropriate number of days completed taking into account: • Multi-site or remote locations? • Change in scope? • Other?	☐	☐	☒
12	Does the audit plan schedule support the audit team NOT doing parallel auditing (i.e., the same auditors for the same process/auditee?	☒	☐	☐
13	If there were CARs from the previous audit was additional time added to the audit plan/schedule to address corrective action implementation/effectiveness?	☐	☐	☒
14	Do the actual audit dates all match on the Draft Report, Final Report, plan/schedule and opening and closing meeting sections?	☒	☐	☐
15	Was the appropriate Audit Summary Matrix for the audit standard (s) audited completed and attached in OASIS? NSF-ISR Asia Pacific auditors should submit the appropriate matirx to the appropriate staff member in the Suzhou, China office.	☒	☐	☐
16	Does it match the client's processes in the Audit Plan/Schedule (11661)?	☒	☐	☐

17	Does the Audit Report include and match all of the client process names listed on the audit plan?	☒	☐	☐
18	For clients with Product Design was the design function audited at least once per 12 month period?	☐	☐	☒
19	If this is a Registration or Reassessment Audit, have all the client processes been audited?	☐	☐	☒
20	Have the opening and closing meeting attendees been recorded and either included in the audit report and/or an attendance list attached in OASIS? NSF-ISR Asia Pacific auditors should submit the opening/closing meeting attendees within the report and/or attendance list to the appropriate staff member in the Suzhou, China office.	☒	☐	☐
21	If there are new locations identified, has the physical address of the location and its specific activities/processes for each location been listed?	☐	☐	☒
22	Are they appropriately identified (i.e., remote location)?	☐	☐	☒
23	Are there clear audit trails that support the relationship between this location and any other location it supports or receives support?	☐	☐	☒
24	Does the audit report clearly show which Customer Specific Requirements were audited?	☐	☐	☒
25	If nonconformance (s) were identified during the audit, then are they clearly written in accordance with the TS/IATF Rules and appropriately graded? Note: For minors, there must be a unique justification for each one – DO NOT “cut & paste.” **TS/IATF ONLY**	☐	☐	☒

26	If OFIs are identified do they include a standard conformance disclaimer, not appear to provide consulting, or be considered a nonconformance?	■	☐	☐
27	Is the recommendation consistent with the results of the audit (e.g., bearing in mind NCRs, customer complaints, customer special status, etc.)?	■	☐	☐
28	For re-assessments was a review performed of the previous cycles data to include past surveillance reports, registration reports, re-assessment reports, and other CB's reports where applicable to identify any adverse trends and documented in the report?	☐	☐	■
29	Has a Draft Report (10132) been emailed to the office within 24 hours of the closing meeting and uploaded in OASIS for this audit? **TS/IATF ONLY** NSF-ISR Asia Pacific auditors should submit the draft report to the appropriate staff member in the Suzhou, China office.	☐	☐	■
30	Have the supplier codes been verified from relevant customer scorecards/documents and confirmed to information within the current FRS?	☐	☐	■
31	If any changes are noted, did you indentify them in the FRS reports section?	☐		■

(End)