Bureau Veritas Certification Holding SAS-UK Branch

ISO/IEC 27001:2013

Audit Report for the 2nd Surveillance Audit Of

Airports of Thailand Public Company Limited

Company Information			
Company Name	Airports of Thailand Public Company Limited		
Company full Address	**HQ - AOT Head Office**, Don Muang, 333 Cherdwutagard Road, Srikan, Don Mueang,Bangkok 10210 ,Thailand **Data Center – AIMS Airport Information Management System (AIMS)**, 999 Moo 1, Bangna - Trad Road Km 15 Rachathewa,Bang Phli Samut Prakan 10540, Thailand **DR Site – Airport Maintenance Facility (AMF)**, 999 Moo 1, Bangna - Trad Road Km 15 Rachathewa,Bang Phli Samut Prakan 10540, Thailand		
Phone No.	66) 2-132-7100	Fax No. / Email-ID	
Website address	https://airportthai.co.th		
Country Name	Thailand		
Contact Information			
Client's Representative	Mr. Somchai Kambumrung	Phone No.	(66) 2-132-7100
Email Address	somchai.k@airportthai.co.th		
ZIG/CONTRACT Number			
Audit Information			
Sector Code	ISC01-IT		
Audit Duration (Mandays)	3.0 MDs	Onsite Audit Duration Offsite Audit Duration	3.0 MDs
No. of Employees	60 persons	No. of Shifts (if yes, please provide shift details)	2 shifts
Audit start date	02 Nov 2020	Audit end date	03 Nov 2020
Next Audit Date (Tentative)	02 Nov 2021	Duration (Mandays)	
Auditor Information			
Team Leader	Mr. Arnut Visawaprasit	Sector Code	ISC01-IT
Team Member 1	Mr. Pongsatorn Waiprasit	Sector Code	ISC01-IT
Team Member 2		Sector Code	
Team Member 3		Sector Code	
Team Member 4		Sector Code	
If this is a multi-site audit an Appendix listing all the relevant sites and/or remote locations has been established and attached to the audit report.			
Distribution	Client Contact / Audit Team /BV Certification office		

Summary of Audit Findings

Number of Non Conformities recorded:	Major:	0	Minor:	0	

Is a follow up audit required?	N	Follow up audit start date		day(s)

Actual follow up date(s)	Start:	End:

Follow-up audit remarks:

Scope of Certification (scope statement must be verified and appear in the space below. For multi-site organisations, site wise scope to be listed)

Site	Scope Statement
AOT Head Office, Don Muang : 333 Cherdwutagard Road, Srikan, Don mueang, Bangkok 10210 ,Thailand	The Information Security Management System applies to Airports of Thailand Public Company Limited's Data Centers, ICT Infrastructure, Information Security Continuity and Controls operated at Head Office and Suvarnabhumi Airport. - Data Center management , IT Operation (Don Mueang)
Airport Information Management System (AIMS): 999 Moo 1, Bangna - Trad Road Km 15 Rachathewa,Bang Phli Samut Prakan 10540, Thailand	Data Center management , IT Operation (Suvanabhumi Airport)
Airport Maintenance Facility (AMF) : 999 Moo 1, Bangna - Trad Road Km 15 Rachathewa,Bang Phli Samut Prakan 10540, Thailand	Disaster recovery site (Suvanabhumi Airport)

Statement of Applicability Version number and release date : rev 00, 20 Jun 2016

Accreditation	UKAS
No. of Certs required	1
Languages	ENGLISH
Reason for Issue of Certificate	n/a

Further Instructions (additonal certificate instruction or information for the office- other than UKAS) :

n/a

Audit Summary

1.A Audit Objectives – Stage 1 Audit

1. To confirm that the management system conforms with all the requirements of the audit standard(s);
2. To confirm that the organization has effectively implemented its planned arrangements;
3. To confirm that the management system is capable of achieving the organization's policies and objectives and evaluation of the ability of the management system to ensure the client organization meets applicable statutory, regulatory and contractual requirements;
4. If applicable to identify areas for potential improvement of the management system.
5. To audit the client's management system documentation;
6. To evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;

7. To review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system;
8. To collect necessary information regarding the scope of the management system, processes and location(s) of the client, and related statutory and regulatory aspects and compliance (e.g. quality, environmental, legal aspects of the client's operation, associated risks, etc.);
9. To review the allocation of resources for stage 2 audit and agree with the client on the details of the stage 2 audit;
10. To provide a focus for planning the stage 2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of possible significant aspects;
11. To evaluate if the internal audits and management review are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for the stage 2 audit.

1.B Audit Objectives – Other Audits

1. To confirm that the management system conforms with all the requirements of the audit standard(s);
2. To confirm that the organization has effectively implemented its planned arrangements;
3. To confirm that the management system is capable of achieving the organization’s policies and objectives and evaluation of the ability of the management system to ensure the client organization meets applicable statutory, regulatory and contractual requirements;
4. If applicable to identify areas for potential improvement of the management system.
5. The purpose of the stage 2 audit is to evaluate the implementation, including effectiveness, of the client's management
system. It shall include at least the following:
a) information and evidence about conformity to all requirements of the applicable management system standard or other
normative document;
b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document);
c) the client's management system and performance as regards legal compliance;
d) operational control of the client's processes;
e) internal auditing and management review;
f) management responsibility for the client's policies;
g) links between the normative requirements, policy, performance objectives and targets (consistent with the expectations
in the applicable management system standard or other normative document), any
applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions.

2. Previous Audit Results

The results of the last audit of this system have been reviewed, in particular to assure appropriate correction and corrective action has been implemented to address any nonconformity identified.

No. of nonconformities from previous audit	Major	0	Minor	0
No. of nonconformities closed	Major	0	Minor	0
No. of nonconformities re-raised	Major	0	Minor	0

This review has concluded that:
- any nonconformity identified during previous audits has been corrected and the corrective action continues to be effective.

2.1 Performance of the ISMS over the previous period of certification

The organization performed ISMS well during the previous period of certification

2.2 Useful comparison with the previous audit findings [as applicable]

The previous audit findings have been addressed by the system.
No current audit finding match with the previous ones.

3. Management System Effectiveness

The audit team conducted a process-based audit focussing on the sigificant aspects, risks and objectives. The audit method used were interviews, observations of activities and review of documentation and records.
The onsite audit was started with an opening meeting which attended by the senior management of the organization.
The audit findings were communicated to the management of the organization during the closing meeting, final conclusion of the audit results and recommendation by the audit team also briefed to the management during the meeting.

3.1 Basic Inputs

The basic detials of the organization which are manpower, sites, addresses are changed from last recertification audit as indentified in the Company Information (above).
The ISMS system of the organization is unchanged from the last recertification audit.

3.2 Description of company activities [mandatory for audits leading to certification decision and/or certificate issuance]

Location :
□ **HQ - AOT Head Office**, Don Muang, 333 Cherdwutagard Road, Srikan, Don Mueang,Bangkok 10210 ,Thailand

□ **Data Center - Airport Information Management System (AIMS)**, 999 Moo 1, Bangna - Trad Road Km 15 Rachathewa,Bang Phli Samut Prakan 10540, Thailand

□ **DR Site – Airport Maintenance Facility (AMF)**, 999 Moo 1, Bangna - Trad Road Km 15 Rachathewa,Bang Phli Samut Prakan 10540, Thailand

- **Key services / activities :** Data center and IT operation for the airport

- **Organization / Business Unit :** ICT steering committee, Internal auditor, ISMS working committee , IT Infrastructure team

- **Number of people within scope :** 60

3.3 Validation of Scope of Certification:[mandatory for all certification, recertification and change of scope audits]

The audit team has validated the scope to Internal and External Context, Needs and Expectation of Interested parties, Interfaces and dependencies between activities of organizationand those that are performed by other orgnaization (supplier, other intereste parties)

3.4 Context of the organizationdation :

External Context	Internal Context
Privacy law, GDPR	Insufficient of technical staff
Cyber threats	
Critical intrastructure	
Technology change	

3.5 Needs & Expectations of the Interested parties:

Interested Parties	Needs & Expectation
Ministry of transport The civil aviation authority of Thailand	- Follow the vision and strategy for the development of information technology. - Comply to the Information and communication technology policy - Operation under good governance - Information facilities and communication systems are available and continuity
Aeronautical – Partner	- IT services are effectiveness and qualified international standard - IT service continuity
Ministry of Finance - share holder	- IT services are effectiveness and qualified international standard - IT service continuity
Subcontractor	- Role and responsibilities is clearly defined
Customer	- Information facilities and communication systems are available and continuity to support IT services 1.
Staff	- Information facilities and communication systems are available and continuity to support IT services - Encourage employees and employees to have sufficient knowledge and skills to perform their work. 1.

3.6 Risks & Opportunities:

Risk and opportunities have been determined as a part of risk assessment methodology, see topic 3.8

3.7 Breifly describes Risk assessment Process :

SD-1608010-002, V.5, 26 Oct'20; ISMS Risk Management Methodology8

Information security risk assessment has been evaluated based on risk scenario. Threats and vulnerabilities of each scenario are defined and evaluate risk level by using the following criteria.

- Risk assessment criteria
  - Impact – 1-5 levels – based on legal, operation, reputation, finance impact.
  - Likelihood --- 1-5 level – (Very low to very high)
  - Risk score = Impact x Likelihood (5x5 matrix)
  - Acceptable risk level = medium

3.8 Breifly describes Risk Treatment Process :

- 2 RTP raised for 4 high risks, as follow:
  - RTP-2563-001 – review Firewall rule to prevent Vulnerbility of Backup system – ongoing (Mar'21)
  - RTP-2563-002 – identify Security requirments for Backup system – ongoing (Apr'21)
- 4 OFI raised for medium risks, as follow
  - OFI-2563-001 – provide ISMS awareness training for Network service – ongoing Apr'21)
  - OFI-2563-002 – DRP test for Network system – ongoing (Sep'21)
  - OFI-2563-003 – review preventive maintenance for Fire Detection/Fire Alarm (AMF) – ongoing (Sep'21)
  - OFI-2563-004 – review computers for new users -- ongoing (Sep'21)

3.9 Statement of Applicability (Exclusions & Justifications):

Statement of Applicability (SOA)					
Document Number:	SD-6121-003	Date:	1/08/2019	Revision:	2.0

SOA Exclusion:			
No. of Exclusion of Controls in Annex A:			9
	Sub-clauses of Annex A, Justification for exclusion		
1.	A.9.4.5	Access control to program source code	Software development is not included within this scope
2.	A.11.2.6	Security of equipment and assets off-premises	Equipment or asset off premises is not allowed
3.	A.14.1.2	Securing application services on public networks	There is not allowed to transfer any information through public network
4.	A.14.1.3	Protecting application services transactions	There is not allowed to transfer any information through public network
5.	A.14.2.2	System change control procedures	Software development is not included within this scope
6.	A.14.2.6	Secure development environment	Software development is not included within this scope
7.	A.14.2.7	Outsourced development	Software development is not included within this scope
8.	A.14.2.9	System acceptance testing	Software development is not included within this scope
9.	A.14.3.1	Protection of test data	Software development is not included within this scope

3.10 Detail of Leadership commitments (scope,participation in Management review, participation in opening closing /meeting,assigning responsibilities and authorities, Resource provision)and Information security objectives and the monitoring of these towards achievement:

- Resources were found to be properly provided to support the implementation of ISMS.
- The management has demonstrated the leadership for ISMS; e.g. establishing and reviewing the ISMS Policy, IS Policies, setting IS Objectives and Performance Target, monitoring and review the Performance Results, participating in Management Review, providing resources.

3.11 Internal and External communication

Communication related to IT security is provided through awareness training, Email

3.12 Verification of each previous BVC audit NCR / Useful comparison with the previous audit findings -

- Previous audit has no NC finding.

3.13 Evaluation of Complaince during shifts (General/first/second/third shifts) and effectiveness of system implementation

The effectiveness of shift operation can be verified through monitoring system and record of daily checklist. For those incident or event which have been found or detect, shift team will report to system admin and team lead directly.

3.14 Internal audits (including degree of reliance that can be placed on this process) :

- Internal Audit Programme
    - Internal audit plan in Sep’20 (1 time/year) to audit at H/O, AIMS, AMF
- Internal Audit Plan 1/2020 on 01-08 Sep’20 (5 days audit) to audit all applicable requirements of ISO 27001:2013. The audit areas are H/O, AIMS Data Center, AMF Data Center
- Internal auditors had re-trained in ISO 27001:2013 Internal Auditor in yearly, on 23 Aug’20 and take exam. By ASIC.
- Internal Audit report
    - 0 major NC
    - 6 minor – raised 6 CARs – ongoing for closing
        1. No C/I/A identify for Risk assessment 2020
        2. No RTP raised for high risks
        3. Risk Management Methodology was not revised according to ISMS committee comment
        4. No access reviewed
        5. NC for Physical access control, CCTV, PC monitoring , and Backup
        6. Physical access control at H/O not comply to the policy
    - 11 OFI – raised 11 CARs – on going for raised CARs
- Internal Audit Checklist identified clause/Annex no., audit trail, audit result (details of comply/NC/OFI)

3.15 Management Review (including degree of reliance that can be placed on this process) :

- 1/2020 Management Review Meeting on 27 Jan’20 with follow agenda:
    - ISMS implementation plan and status
    - Corrective action for Internal audit in 2019
    - Risk treatment plan 2019 status
    - ISMS effectiveness monitoring status
    - Critical security incident
    - 1st Surveillance audit result
    - ISMS plan 2020
    - Risk management scope
    - Last meeting follow up
    - ISMS communications
    - ISMS Management review
    - ISMS committee meeting plan
- 2/2020 Management Review Meeting on 31 Aug’20 with follow agenda:
    - ISMS implementation status
    - ICT organization changed and ISMS
    - ISMS effectiveness monitoring 2020 status
    - Risk Treatment Plan 2020 status
    - Internal audit 2020 status
    - Internal audit 2020 plan
    - CB audit plan 2020
    - ISMS Risk assessment 2020
    - Document review in 2020
    - ICT Security policy review
    - Last meeting follow up
    - Critical Security Incident
    - ISMS awareness
    - ISMS PR

    - ISMS Management Review
    - ISMS Committee meeting plan
- 3/2020 Management Review meeting on 28 Oct'20 with follow agenda:
    - Agenda are same as above meetings, update details.
- No use of UKAS logo.

3.16 Non conformity and Corrective action effectiveness

- 6 CARs are raised for NCs of Internal Audit on 01-08 Sep'20 – ongoing (to be closed within 90 days (Dec'20))
- 11 CARs are raised for OFIs of Internal Audit on 01-08 Sep'20 – ongoing (to be closed within 365 day)
- CARs of last year Internal audit are closed (NC/OFI)

3.17 ISMS Documentation

Document Review Item	Compliant (Yes/No)	Comments (Revision number & Date of release)
4.3 Scope of the ISMS	***Yes***	***SD-1608010-001, V.6, 26 Oct'20***
5.2 Information security policy	***Yes***	***GU-6121-001, V.1, 1 Oct'18***
6.1.2 Information security risk assessment process	***Yes***	***SD-1608010-002, V5, 26 Oct'20***
6.1.3 Information security risk treatment process	***Yes***	***SD-1608010-002, V5, 26 Oct'20***
6.1.3 d) Statement of Applicability	***Yes***	***SD-1608010-003, V.4, 1 Sep'20***
6.1.3 e) Risk treatment plan	***Yes***	***SD-1608010-002, V5, 26 Oct'20***
6.2 Information security objectives	***Yes***	***SD-1608010-005, V.4, 28 Aug'20***
7.2 Evidence of competence	***Yes***	Evidence of competence of each staff are available and maintain by HR .
7.3 Evidence of awareness	***Yes***	Evidence of competence of each staff are available and maintain by HR .
7.5.1 b) Documented information determined by the organization as necessary for the effectiveness of the ISMS	***Yes***	Management review meetings are shown effectiveness monitoring updated for each meeting.
8.1 Documented information to the extent necessary to have confidence that the processes have been carried out as planned	***Yes***	Internal audit shown that the processes have confidence that the processes have been carried out as planned.
8.2 Results of the information security risk assessments	***Yes***	***SD-1608010-004, V.4, 28 Oct'20***
8.3 Results of the information security risk treatment	***Yes***	***SD-1608010-004, V.4, 28 Oct'20***
9.1 Evidence of the monitoring and measurement results	***Yes***	Management review meetings are shown effectiveness monitoring updated for each meeting.
9.2 g) Evidence of the audit programme(s) and the audit results	***Yes***	Internal audit plan in Sep'20
9.3 Evidence of the results of management reviews	***Yes***	***Management review meeting 1/20, 2/20, 3/20***
10.1 f) Evidence of NCR nature and subsequent actions taken	***Yes***	***See topic no. 3.16***
10.1 g) Evidence of the results of any corrective action	***Yes***	***See topic no. 3.16***

3.18 Compliance to ISMS related legal and regulatory requirements :

List of Applicable Legal & Regulatory Requirements	Compliant (Yes/No)	Comments
Computer Related Crime Act 2007	***Yes***	
Official Information act 1997	***Yes***	
Copyright Act 1994	***Yes***	
Electronic transaction law 2008	***Yes***	
Cyber Security Act 2019	***Yes***	
Privacy and Protection of Personality Identification Act 2019	***Yes***	

3.19 Best Practices

Staffs Competency and co-operated

3.20 Opportunities for Improvement

- none

3.21 Observation (Potential Non Conformity)

- none

3.22 Agreed follow-up actions [if NCR pending]:

- n/a

3.23 Non-conformities

Non conformities detailed herein shall be addressed through the organization's corrective action process, in accordance with the relevant corrective action requirements of the audit standard.

Hereunder you will find Bureau Veritas Certification requirements for:

- *expected timelines to address the nonconformity (a)*
- *response content (b)*

Expected timelines to address the non-conformity (a)

Corrections and Corrective actions (if possible) to address identified major nonconformities shall be carried out immediately. Correction, Root Cause Analysis and Corrective action plan together with satisfactory evidences of implementation shall be submitted within 90 days after the last day of the audit unless Bureau Veritas Certification and client agree on a longer period of time.

Review of nonconformities is done through desktop review. However, depending of severity of the findings, our auditor may perform a follow up visit to confirm the actions taken, evaluate their effectiveness, and determine whether certification can be recommended or continued.

For a minor nonconformity, correction, root cause analysis and corrective action plan shall be approved by the team leader and verification of implementation and effectiveness of corrective action(s) taken will be performed at the next visit.

It is recommended that the Client provide responses early to allow time for additional reviews if needed.

For recertification time limits to address nonconformities will be defined by the team leader in order to have them implemented prior to expiration of certification.

Any responses to the nonconformities which were raised may be either in hard copy or electronically using the NCR herein (preferred) and forwarded to the Bureau Veritas Certification office.

Expected response content (b)

Client response to NCR should be reviewed by the lead auditor in three parts; correction, RCA and corrective actions.

In reviewing the three parts, the auditor looks for a plan and then evidence that plan is being implemented.

Correction

1. The extent of the nonconformity has been determined (NCR has been corrected & the client has examined the system to see if there are other examples that need to be corrected). Ensure that correction answers the question "Is this isolated case or not?" in other words "Is there a risk that this can reoccur at the other site / department?"

2. If correction cannot be immediate; a plan to correct the NCR may be appropriate (responsible & date).

3. Evidence that the correction was implemented or evidence that the plan is being implemented.

Root Cause Analysis

1. The Root Cause is not simply repeating the finding, neither is the direct cause of the issue.

2. Well thought out analysis to determine the true root cause: e.g. someone did not follow a process would be direct cause; determining why someone did not follow a process would lead to the true root cause.

3. The root cause statement must focus on a single issue without any obvious """""""""""""why""""""""""""" questions remaining.

If a """""""""""""why""""""""""""" question can reasonably be asked about the root cause analysis, this indicates that the analysis did not go far enough.

4. Ensure that the root cause answers the question, "What in the system failed such that the problem occurred?"

5. Blaming the employee will not be accepted as the only root cause

6. Address problems with the process as well as what detection system failed

Corrective Action

1. The corrective action or corrective action plan addresses the root cause(s) determined in the root cause analysis. If you have not defined true root cause you cannot prevent the problem from its reoccurrence

2. In order to accept the plan it shall include;

- *actions to address the root cause(s)*
- *identification of responsible parties for the actions and*
- *a schedule (dates) for implementation.*
- *always include a "change" to your system. Training and/or publishing a newsletter are generally not changes to your system*

3. In order to accept the evidence of implementation:

a. Enough evidence is provided to show the plan is being implemented as outlined in the response (and on schedule).

b. Note: Evidence in full is not required to close the NCR; some evidence may be reviewed during future audit when verifying the corrective actions.

3.24 Comment on usage of Logo

- No use of UKAS logo.

3.25 Comment on Allocation of Resources for Stage 2 (applicable only in Stage 1 audit).

- **n/a**

4. Review of Performance for Current Certification Cycle (Last Surveillance)

- **The organization performed well in ISMS.**

5. Team Leader Recommendation

The audit team conducted a process-based audit focussing on significant aspects/risks and objectives required by the standard(s). The audit methods used were interviews, observations, sampling of activities and review of documentation and records.

- Maintain Certification

This report is confidential and distribution is limited to the audit team, Client and BV local Certification entity.

AUDIT SUMMARY REPORT FOR ISO 27001:2013

Process Name			
Process 1	Nov 02, 2020		
Process 2	Nov 02, 2020		
Process 3	Nov 02, 2020		
Process 4	Nov 03, 2020		
Process 5	Nov 03 2020		
Process 6	Nov 03, 2020		

		Doc Rev Compliant (Y/N)	Process / Acivity / Department Process 1: H/O: Context of Organization, Interested Parties, Scope, Risk Management, Management Review, Internal Audit, Information Security Performance and Effectiveness, Compliance	Process 2: H/O: Management Review, Intenrla Audit, Correcticve Action, Document and Record Control, Information Classifcation, Labelling,	*Process 3: H/O: Physical and Envifronmental Securit, Operation Security, Network Security, Human Resource Security, Awareness Training*	Process 4: AMS: Physical and Environmental Security, Operation Security, Network Security, Incident and Change Managment	Process 5: AMF: DR Site visit, including DR plan and Exercise result.	Process 6: AIMS: Facility Management, Supplier Relationships	NCR TOTALS
	CLAUSES								
Clause	Description								
4.1	Understanding the organization and its context	Y	X						
4.2	Understanding the needs and expectations of interested parties	Y	X						
4.3	Determining the scope of the information security management system	Y	X						
4.4	Information security management system	Y	X						
5.1	Leadership and commitment	Y	X						
5.2	Policy	Y	X						
5.3	Organizational roles, responsibilities and authorities	Y	X						
6.1.1	Actions to address risks and opportunities - General	Y	X						
6.1.2	Information security risk assessment	Y	X						
6.1.3	Information security risk treatment	Y	X						
6.2	Information security objectives and planning to achieve them	Y	X						
7.1	Resources	Y							
7.2	Competence	Y							
7.3	Awareness	Y							
7.4	Communication	Y	X						
7.5	Documented information	Y	X						
8.1	Operational planning and control	Y	X						
8.2	Information security risk assessment	Y	X						
8.3	Information security risk treatment	Y	X						
9.1	Monitoring, measurement, analysis and evaluation	Y		X					
9.2	Internal audit	Y		X					
9.3	Management review	Y		X					
10.1	Nonconformity and corrective action	Y		X					
10.2	Continual improvement	Y		X					
A 5	Information security policies	Y							
A 6	Organization of information security	Y							
A 7	Human resource security	Y							
A 8	Asset management	Y			X	X	X		
A 9	Access control	Y			X	X	X		
A 10	Cryptography	Y			X	X	X		
A 11	Physical and environmental security	Y			X	X	X	X	
A 12	Operations security	Y			X	X	X		

A 13	Communications security	Y			X	X			
A 14	System acquisition, development and maintenance	Y			X	X			
A 15	Supplier relationships	Y						X	
A 16	Information security incident management	Y				X			
A 17	Information security aspects of business continuity management	Y					X		
A 18	Compliance	Y	X						
	Use of Logo’s	Y	X						0