LAPORAN KEGIATAN AUDIT SURVEILLANCE

SMKI ISO 27001:2022

INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR

TANGGAL 05 JULI 2024
TAHUN ANGGARAN 2024

+62 823-2801-9993
www.mitrasejatifazahara.com
Jl. Indraprasta No. 8A RT 02 RW 26,
Pringgolayan Dabag, Condongcatur,
Sleman, Daerah Istimewa Yogyakarta.

LAPORAN KEGIATAN AUDIT SURVEILLANCE SMKI ISO 27001:2022
INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR
TANGGAL 05 Juli 2024
TAHUN ANGGARAN 2024

DAFTAR ISI

LAPORAN KEGIATAN AUDIT SURVEILLANCE SMKI ISO 27001:2022
INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR
TANGGAL 05 Juli 2024
TAHUN ANGGARAN 2024

A. LATAR BELAKANG

Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan mengintegrasikan pada SMM ISO 9001:2015, SMKI ISO 27001:2022 dan SMAP ISO 37001:2016 merupakan surveillance integrasi dari tiga standar Internasional dalam manajemen organisasi yang sasaran kinerjanya adalah memberikan parameter internasional dalam penyelenggaraan pelayanan public. Manajemen organisasi sejatinya harus setiap waktu dan setiap saat melakukan peningkatan pelayanan dan memperbaiki secepat-cepatnya jika adanya ketidaksesuaian dalam sistem mauapun implementasi layanannya. Pelayanan publik dan manajemen organisasi ditunjukkan pada sistem pemerintahan agar lebih efektif dan efisien serta memiliki kualitas sumber daya manusia aparatur menjadi lebih unggul dan dapat menjawab semua keinginan dan harapan pemangku kepantingan. Hal ini juga ditunjukkan dari masih banyaknya keluhan dan pengaduan dari masyarakat baik secara langsung maupun melalui media massa, elektronik dan social, berkaitan dengan prosedur yang berbelit-belit, tidak ada kepastian dalam jangka waktu penyelesaian, biaya yang harus dikeluarkan, persyaratan yang kurang transparan, sikap petugas yang kurang responsif dan lain-lain. Sehingga berpotensi menimbulkan citra yang kurang baik terhadap pelayanan pemerintah dimata masyarakatnya sendiri, terutama masyarakat awam yang belum terlalu memahami tentang pelayanan publik. Sistem Manajemen Mutu 9001:2015 merupakan salah satu pedoman dengan persyaratan pemenuhannya dalam tata kelola organisasi.

Implementasi dari manajemen terintegrasi dalam organisasi agar tercapai pelayanan prima yang berkelanjutan dilingkungan aparatur Provinsi Nusa

Tenggara Timur, maka diterapkan Standar Sistem Manajemen Mutu ISO 9001:2015; Sistem Manajemen Keamanan Informasi ISO 27001:2022 dan Sistem Manajemen Anti Penyuapan ISO 37001:2016.

Adapun rangkaian kegiatan pekerjaan audit integrasi penerapan Sistem Manajemen Terintegrasi SMM, SMKI dan SMAP adalah sebagai berikut:

I. **Registrasi,** kegiatan pendaftaran Inspektorat Daearah Provinsi NTT kepada badan sertifikasi SIS CERTIFICATION INDONESIA dengan melampirkan persyaratan dokumen terintegrasi yang sebelumnya telah dilakukan paparan pemahaman integrasi sistem antara lain;

1. Profil Inspektorat Daerah Provinsi NTT
2. Identifikasi isu – isu internal dan eksternal
3. Risk Management Plan (RMP; BRA; IRS)
4. Identifikasi Kebutuhan dan Harapan Pemangku Kepentingan
5. Analisa SWOT
6. Bisnis Proses Organisasi

Tujuan & Hasil Yang Diharapkan:

Organisasi yang terregistrasi dapat melanjutkan pada tahap selanjutnya yaitu *document review* (stage 1) proses integrasi sistem.

II. **Audit Stage 1 (*Document Review*),** kegiatan yang dilakukan oleh badan sertifikasi untuk memastikan bahwa kelengkapan dokumen persyaratan telah terpenuhi dan dapat melanjutkan pada tahap audit integrasi dengan mengunjungi secara langsung atau Audit Stage 2.

Tujuan & Hasil Yang diharpakan:

Pada tahap ini, organisasi yang lulus pada tahap stage 1 ini, akan direkomendasikan pada tahap selanjutnya yaitu audit sertifikasi (stage 2).

III. **Audit Stage 2 (*Audit Certification*),** kegiatan yang dilakukan oleh badan sertifikasi SIS CERTIFICATION (*on-site*), untuk memeriksa, mengukur dan mengevaluasi secara langsung dengan bukti-bukti obyektif berdasarkan persyaratan yang ada di Sistem Manajemen Terintegrasi SMM, SMKI &

SMAP. Keputusan layak dan tidaknya organisasi ditentukan oleh proses yang ada di Stage 2 ini.

Tujuan & Hasil Yang Diharapkan:

Pada tahap ini audit dilakukan sesuai persyaratan yang ada didalam Sistem Manajemen Terintegrasi SMM, SMKI & SMAP dan diberikan rekomendasi lulus dari laporan hasil audit integrasi dan kemuadian jika sudah ada tindaklanjut jika ada temuan yang harus diperbaiki maka akan direlease Sertifikat ISO 9001:2015; ISO 27001:2022 & ISO 37001:2016.

B. TUJUAN DAN KONTRAK KERJA

Tujuan laporan kegiatan ini adalah untuk melaporkan pelaksanaan Audit Surveillance Sistem Manajemen Terintegrasi SMM, SMKI & SMAP kepada **INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR** sampai dengan 100% pekerjaan selesai sesuai dengan rencana yang telah ditetapkan baik mengenai waktu pelaksanaan maupun cakupan pekerjaannya, berdasarkan pada **Surat Perjanjian Kontrak Nomor: SPK-ITDA/02/VII/2024 Tanggal 04 Juli 2024, dengan Nilai Kontrak Kerja adalah: Rp. 28.860.000,00 (Dua Puluh Delapan Juta Delapan Ratus Enam Puluh Ribu Rupiah)**

C. RUANG LINGKUP PEKERJAAN

Ruang lingkup Pekerjaan Audit Surveillance SMKI ISO 27001:2022 yang pelaksanaannya dilakukan secara terintegrasi SMM, SMKI & SMAP Provinsi Nusa Tenggara Timur Tahun Anggaran 2024 ini meliputi:

1. RUANG LINGKUP WILAYAH / AREA PEKERJAAN

Ruang lingkup wilayah / area pekerjaan yang pada proses Audit Surveillance Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan terintegrasi SMM, SMKI & SMAP pada Inspektorat Daearah Provinsi NTT Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur 85111.

2. RUANG LINGKUP TAHAPAN PEKERJAAN

Pekerjaan Audit Surveillance Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan pelaksanaan terintegrasi SMM, SMKI & SMAP Inspektorat Daerah Provinsi Nusa Tenggara Timur Tahun Anggaran 2024 terdiri dari :

a. Tahapan Registrasi Audit Surveillance Integrasi,
b. Tahapan Pelaksanaan Audit Surveillance Integrasi,
c. Tahapan Laporan Audit Surveillance Sistem Manajemen Terintegrasi SMM, SMKI & SMAP,
d. Sertifikat lulus Sistem Manajemen Terintegrasi SMM, SMKI & SMAP

D. WAKTU PELAKSANAAN KEGIATAN

Pelaksanaan Kegiatan Audit Surveillance Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan terintegrasi SMM, SMKI & SMAP Provinsi Nusa Tenggara Timur Anggaran 2024 ini dimulai tanggal 05 Juli 2024

E. PEMBAHASAN PELAKSANAAN KEGIATAN

1. Registrasi Audit Su Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan terintegrasi SMM, SMKI & SMAP.

Pada proses ini merupakan pendaftaran kepada **Badan Sertifikasi SIS CERTIFICATION INDONESIA**

2. Pelaksanaan Audit Surveillance Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan terintegrasi SMM, SMKI & SMAP.

Tahap ini Auditor melakukan audit proses dan implementasi pada setiap proses yang masuk dalam ruang lingkup organisasi yang akan sertifikasi Audit Sistem Manajemen Terintegrasi SMM, SMKI & SMAP. Metode yang digunakan dalam Audit adalah wawancara/ interview, sistem informasi terdokumentasi dan observasi terhadap semua Pejabat struktural dan staf pelaksana proses antara lain:

a. Inspektuer Inspektorat Daerah Provinsi NTT (sebagai top manajemen)
b. Pejabat Struktural maupun Fungsional yang berkaitan
c. Staf pendukung lainnya.

Audit Audit Sistem Manajemen Terintegrasi SMM, SMKI & SMAP tanggal 04-05 Juli dan 13 Agustus 2024. Kegiatan Audit Sistem Manajemen Terintegrasi SMM, SMKI & SMAP meliputi:

a. Opening Meeting (Rapat Pembukaan)
   Saat opening meeting Auditor menyampaikan tujuan audit, metode audit dan ruang lingkup penerapan audit dan kategori temuan audit.
b. Metode Audit
   Auditor menyampaikan metode audit yang digunakan saat audit yanitu wawamcara dan pengamatan pada area kerja maupun operasional kerja di semua bagaian sesuai struktur organisasi yang ditetapkan
c. Kategori Audit
d. Auditor menyampaikan kategori temuan audit yaitu:
   i. NC – Major (tidak memenuhi kriteria audit)
   ii. NC – Minor (belum terpenuhi salah satu atau keliru)
   iii. Observasi (saran-saran OFI/ *Opportunity for Improvement*)
e. Closing Meeting (Rapat Penutupan)
   Saat closing meeting, Auditor menyampaikan temuan audit yang telah dilaksanakan secara langsung kepada seluruh Auditee di organisasi dan jika ada kategori NC – Major atau NC – Minor, maka Auditee diberikan kesempatan melengkapi ***NCCAP (NON-CONFORMANCE CORRECTIVE ACTION PLAN)*.**

3. Laporan Audit Sistem Manajemen Keamanan Informasi ISO 27001:2022 Terintegrasi SMM, SMKI & SMAP

Tahap ini Auditor menyampaikan laporan hasil audit berupa temuan hasil audit dan tindak lanjut yang harus dilaksanakan oleh penanggung jawab proses di organisasi yaitu kategori:

1. **Temuan kategori Major**, yaitu ketidaksesuaian dan bertentangan dengan persyaratan Sistem Manajemen Terintegrasi SMM, SMKI & SMAP, maupun standar kerja yang ditetapkan oleh organisasi (SOP), serta regulasi atau peraturan kebijakan dari pemangku kepentingan yang relevan dan berpotensi berdampak fatal bagi organisasi
2. **Temuan kategori Minor**, yaitu kesalahan, kekeliruan atau belum secara lengkap memahami dan belum berdampak fatal bagi organisas

3. **Saran – saran praktis (OFI, *opportunity for improvement*)**, merupakan saran agar peningkatan organisasi menjadi lebih baik dan berinovasi dalam manajemen mutu serta kinerja organisasi

Auditor mengirimkan ***NCCAP (NON-CONFORMANCE CORRECTIVE ACTION PLAN),*** dan memberi kesempatan 2 minggu untuk membuat rencana tindak lanjut temuan audit apabila ada temuan kategori Major dan Minor, sedangkan kategori OFI akan dialakukan verifikasi pada audit surveillance setahun kemudian termasuk evaluasi konsistensi dari temuan kategori Major dan Minor.

4. Sertifikat Sistem Manajemen Keamanan Informasi ISO 27001:2022 terintegrasi SMM, SMKI & SMAP

Badan Sertifikasi (SIS CERTIFICATION), menerbitkan sertifikat asli dan pada setiap kegiataan surveillance setiap tahun akan diperbaharui sesuai dengan waktu surveillance setelah 12 bulan dari tahap sertifikasi, adapapun proses tersebut sebagai berikut:

1) Sertifikat hasil sertifikasi, yaitu tahap audit sertifikasi pertama
2) Sertifikat hasil surveillance 1, yaitu 12 bulan setelah pelaksanaan sertifikasi bertujuan untuk mengukur konsistensi hasil perbaikan, peningkatan, inovasi dan evaluasi terhadap saran-saran yang diberikan oleh auditor termasuk jika terjadi perubahan ruang lingkup sertifikasi
3) Sertifikat hasil surveillance 2, yaitu 24 bulan setelah pelaksanaan sertifikasi bertujuan untuk mengukur konsistensi hasil perbaikan, peningkatan, inovasi dan evaluasi terhadap saran-saran yang diberikan oleh auditor termasuk jika terjadi perubahan ruang lingkup sertifikasi
4) Recertification (re-sertifikasi), yaitu 36 bulan setelah pelaksanaan sertifikasi, bertujuan untuk melakukan evaluasi secara menyeluruh dan kelanjutan proses sertifikasi Sistem Manajemen Terintegrasi SMM, SMKI & SMAP di organisasi

F. PENUTUP

Pelaksanaan kegiatan Audit Surveillance Sistem Manajemen Keamanan Informasi ISO 27001:2022 dengan penerapan Sistem Manajemen Terintegrasi SMM, SMKI & SMAP di Inspektorat Daerah Provinsi Nusa Tenggara Timur Tahun Anggaran 2024 dilaksanakan selama 3 hari, penyelesaian tindakan perbaikan terhadap temuan maksimal 2 minggu, proses verifikasi dan evaluasi hasil perbaikan Badan Sertifikasi SIS CERTIFICATION maksimal 4 Minggu, total pekerjaan adalah 45 hari kerja sampai sertifikat asli dikeluarkan oleh Badan Sertifikasi SIS CERTIFICATION.

Seluruh tahapan kegiatan telah dilaksanakan meliputi: Registrasi Audit Surveillance Integrasi Sistem Manajemen SMM, SMKI & SMAP, Pelaksanaan Audit Surveillance Integrasi Sistem Manajemen SMM, SMKI & SMAP, Laporan Audit Surveillance Integrasi Sistem Manajemen SMM, SMKI & SMAP dan Sertifikasi Audit Surveillance Integrasi Sistem Manajemen SMM, SMKI & SMAP sesuai jadwal serta berjalan lancar.

Semoga kegiatan audit sertifikasi yang telah terlaksana ini, harapannya tidak hanya sampai organisasi dinyatakan layak tersertifikasi saja, akan tetapi Sistem Manajemen Sistem Manajemen Terintegrasi SMM, SMKI & SMAP dapat membudaya di lingkungan organisasi Inspektorat Daerah Provinsi Nusa Tenggara Timur.

Demikian laporan ini kami sampaikan, semoga dapat memberikan manfaat bagi semua pihak yang membutuhkan.

Yogyakarta, 03 September 2024

CV. Mitra Sejati Fazahara

Ivar Kusradi Drajat, ST., M.Eng

Direktur

LAMPIRAN

SURAT TUGAS AUDITOR

No.: 002/SISCERTIND/MSFYK/VII/2024

Yang bertanda tangan di bawah ini **Representative Official Head SISCERT Indonesia** menugaskan kepada:

Nama	: **Ivar Kusradi. D, ST., M.Eng**
Jabatan	: Lead Auditor (Ketua Tim Auditor)
Keperluan	: Melaksanakan tugas sebagai **Lead Auditor** dalam rangka **Audit Surveillance SMKI ISO 27001:2022**
Hari/ Tanggal	: 05 Juli 2024
Tempat/ Organisasi	: **Inspektorat Daerah Provinsi NTT** Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur 85111

Dr. Arfanda Anugrah Siregar. ST., M.Si
Rep. Official & Expert Siscert Indonesia

SIS Certifications

Date: 01.07.2024

Client Reference **No. 001/MSFYK/INT.-27K/VII/2024**

Client Name : **INSPEKTORAT DAERAH PROVINSI NTT**
Head office : **Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur 85111**
Worksite : **Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur 85111**
Head of org : **Mr. Stefanus F. Halla., ST. MM**

STANDARD NAME: ISMS ISO 27001:2022

We would like to confirm that the above-mentioned has been scheduled for the date **05 July, 2024**. The Lead Auditor is **Mr. Ivar Kusradi. D. ST., M.Eng**. Kindly ensure that the activities per the scope are in operation and can be verified during the audit.

Please let us know of any changes to agree audit dates in advance.

Yours Sincerely,

Ivar Kusradi. D. ST., M.Eng
Lead Auditor SISCERT

Unit No. 514, 5th Floor,Vipul Business Park, Sohna Road, Sector – 48, Gurgaon-122018, Haryana, India.

SIS Certifications

We Do Not Sell, We Certify!

AUDIT PLAN		
SR. NO.	**PARTICULAR**	**DESCRIPTION**
1	Name of audited organization	**INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR**
2	Certified Location	Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur 85111
3	Lead Auditor	Ivar Kusradi. D. ST., M.Eng
4	Auditor	NA
5	Technical Expert	NA
6	Standard	**ISO 27001:2022**
7	Standard /criteria/Objective	☐ Stage 1: To audit the management system documentation and determine preparedness for Stage 2. ☐ Stage 2, **Surveillance**, Recertification: To evaluate implementation and effectiveness of the management system. To determine whether the company's management system conforms with the criteria stated below, is able to ensure that applicable statutory, regulatory and contractual requirements can be met, is effective in ensuring that specified objectives are continually met and areas for potential improvement are continually met, where possible The following reference standard: ISO 19011:2018: Guidelines for auditing management systems IAF MD 4:2018 Remote auditing (if remote Audit) IAD ID 3:2011 Management of Extraordinary Events or Circumstances Affecting ABs, CABs and Certified Organizations (if remote Audit) The company's management system processes and documentation

8	Scope of Certification	**Specialized Agencies of the Regional Bodies for Performance Assessment and Development**													
9	Sector Code	EA 36													
10	Language used during audit	INDONESIAN													
11	Type of Audit	Individual		Combined		Joint		Integrated		On-site		Remote			
12	Stage of Audit	Stage I		Stage II		**Surveillance** No. _____		**Recertification**		Transfer		Transition			
13	Date(s) of audit	July, 5th, 2024													

Date: July, 5th, 2024

Date/Day	Time	Activity/ Process/ Function	Clauses	Auditee (s)	Auditor(s)
Day 1 (July, 4th, 2024)	**09.00 – 09.30**	**OPENING MEETING**		**ALL**	IVAR KUSRADI. D. ST. M.Eng.
	09.30 – 10.00	**Interview Inspektur Inspektorat Daerah Prov. NTT** (i.e., Penjelasan Ringkas; Kebijakan, Sasaran & Capaian Integrasi Sistem Manajemen SMM, SMKI & SMAP)	**All clause & Annex (SoA - SMKI ISO 27001:2022) & ISO 37001:2016**	**Inspektur**	
	10.00 – 12.00	**Materi Audit Resertifikasi & Surveillance1 Koordinator & Tim Integrasi SMKI & SMAP i.e.,** 1. Internal Audit Integrasi (SMKI, SMAP) (cl. 9.2) 2. Rapat Tinjauan Manajemen Integrasi (cl. 9.3) 3. Pernyataan Kebijakan Manajemen Integrasi (SMKI, SMAP) termasuk Sasaran dan Capaian (A.5, cl. 6.2) 4. Analisa Risiko/ Risk Management Plan Integration (SMKI, SMAP) (cl. 6.1, cl. 6.3)		**Koordinator & Tim Integrasi Sistem (SMM, SMKI & SMAP)**	IVAR KUSRADI. D. ST. M.Eng.
	12.00 – 13.00	**Break (Istirahat/ Makan Siang)**			

	13.00 – 14.30	**Materi Audit Resertifikasi & Surveillance1 Koordinator & Tim Integrasi SMKI & SMAP i.e.,** 5. Pengendalian interaksi fisik, lingkungan dan pembatasan area, ruang komunikasi dan pemantauan, instalasi server, pengkabelan dan tata letak, utilitas pendukung, pemeliharaan dan pemindahan alat, media dan lainnya (SMKI & SMAP) 6. Inventarisasi asset informasi (termasuk asset informasi bergerak, fixed asset, penyimpanan, pemusnahan & media) dan pengendaliannya (SMKI & SMAP) 7. Pengendalian Akses Informasi dan Jaringan (pembagian akses, penggunan dan kendali) (SMKI 8. Pengendalian Informasi Terdokumentasi & sistem kearsipan i.e., *Kebijakan, Pakta Integritas (SMKI & SMAP), Dokumen Pedoman Pelaksanaan Integrasi SMKI & SMAP i.e., issues, SWOT analysis, capaian & kinerja manajemen terintegrasi, SOP, daftar peraturan/ regulasi yang relevan dengan SMKI, SMAP, dan lainnya.)* (cl. 4.1, cl. 6.1, cl. 7.5)	**All clause & Annex (SoA - SMKI ISO 27001:2022) & ISO 37001:2016**	**Koordinator & Tim Integrasi Sistem (SMM, SMKI & SMAP)**	IVAR KUSRADI. D. ST. M.Eng.
	14.30 – 15.00	**Offices tour and Physical and Environment Security Survey (Survey Head Office and Facilities Areas)**	**All clause & Annex (SoA - SMKI ISO 27001:2022) & ISO 37001:2016**	**Koordinator & Tim Integrasi Sistem (SMM, SMKI & SMAP)**	**IVAR KUSRADI. D., ST., M.Eng.**
	15.00	**END of AUDIT DAY 01**			

Day 2 (July, 4th, 2024)	09.00 – 12.00	**Lanjutan, Materi Audit i.e.,** 9. Keamanan operasional i.e., penggunan anti-virus, sistem operasi, pemasangan/ intalasi aplikasi dan perubahan (up-grade system serta kebijakan pengendaliannya), pencadangan/ back up data system serta pengujian-nya 10. Peningkatan kemampuan pegawai teknis dan non teknis berbasis kompetensi (SMKI, & SMAP) 11. Akuisisi dan pengembangan aplikasi, Kerjasama eksternalk pengembangan, rekayasa sistem serta pengujian aplikasi dan implementasinya (data uji) 12. Pengendalian UPG (Pengelolaan Gratifikasi)/ SMAP 13. Pengendalian WBS/ raising concern/ pelaporan upaya suap dan prosedur/ kebijakan (Wistle Blower System)/ SMAP 14. Uji Kepatutan terhadap pihak-pihak internal & eksternal yang terlibat dalam suatu pekerjaan (due diligence)/ SMAP 15. Penanganan & Manajemen insiden dan pedoman/ prosedur i.e., identifikasi, analisa sebab, dan tindaklanjut perbaikannya pada sistem keamanan informasi, dan anti penyuapan serta mitigasi risiko	All clause & Annex (SoA - SMKI ISO 27001:2022) & ISO 37001:2016	IVAR KUSRADI. D., ST., M.Eng.
	12.00 – 13.00	**Break (Istirahat/ Makan Siang)**		
	13.00 – 14.00	**Offices tour and Physical and Environment Security Survey (Survey Head Office and Facilities Areas)**	All clause & Annex (SoA - SMKI ISO 27001:2022) & ISO 37001:2016	IVAR KUSRADI. D., ST., M.Eng.
	14.00 – 15.00	**CLOSING MEETING**		
	15.00	**END of AUDIT**		

Program Elaborated by
Date: 05.07.2024

Ivar Kusradi, D. ST., M.Eng
Lead Auditor SISCERT

Program Accepted by

Stefanus F. Halla., ST. MM
plt. INSPEKTUR

Unit No. 514, 5th Floor,Vipul Business Park, Sohna Road, Sector – 48, Gurgaon-122018, Haryana, India.

General Guidelines:

The audit plan should cover or reference the following:

- The audit objectives;
- The audit scope, including identification of the organizational and functional units, as well processes to be audited;
- The audit criteria, as well as processes to be audited;
- The audit criteria and any reference documents;
- The locations, dates expected time and duration of audit activities to be conducted, including meeting with auditee' s management;
- The audit methods to be used, including the extent to which audit sampling is needed to obtain sufficient audit evidence and the design of the sampling plan, if applicable;
- The role and responsibilities of audit team members, as well as guided and observers;
- The allocation of appropriate resources to critical area of the audit;
- Considering the applicable statement of applicability within the department and function;
- Identification of auditee's representatives for the audit;
- The working and reporting language of the audit where this is different from the language of the auditor or the auditee or both;
- The audit report topics;
- Logistics and communication arrangements;
- Specific arrangements for the locations to be audited;

- Any specific measures to be taken to address the effect of uncertainty on achieving the audit objectives;
- Matters related to confidentiality and information security;
- Any follow-ip action a previous audit;
- Any follow-up activities to the planned audit and coordination with other audit activities, in case of a joint audit.
- Times given above depend on availability of company staff, documents, records, etc.
- Full day audit must be at least 8 hours & half day audit must be at least 4 hours excluding lunch.
- We reserve the right to modify the programme during the course of the audit if so required to obtain the evidence needed, but would endeavor to keep company informed in such circumstances.
- Audit plan provided above serves as guidance only as it is subjected to change if it deems necessary by the auditors during audit.
- Auditors will aim to speak to management and staff at, or near to, their workplace, where practicable.
- Please provide a guide for each auditor during the visit to accompany him/her on the premises and observe the proceedings.
- Lunch time (for full day audit) is planned on 1300-1400 each day, but can be flexible according to the site.
- Company management and staff are welcome to attend opening meeting, review meetings and closing meeting.

- We look forward to working with you in a positive relationship and assisting you in the improvement of your activities.
  - Although the audit plan identifies the related clauses of the Standard/s under each function / area (especially IMS audit), audit must be carried out based on risk-based & process-based audit approach.
  - The audit plan may be reviewed and accepted by the audit client, and should be presented to be auditee well in advance with a copy to SIS Certifications, head office.
  - Any objection by the auditee to the audit plan should be resolved between the audit team leader, the auditee and the audit client prior to the audit.

PROSES AUDIT SURVEILLANCE SMKI ISO/IEC 27001:2022


INSPEKTORAT DAERAH
PROVINSI NTT


INSPEKTORAT DAERAH
PROVINSI NTT

STATEMENT OF CONFORMITY

Number: 044/IMS/MSF-SISCERT/VII/2024
Date: July 05, 2024

Herewith, we would like to notify that:

Organization Name	:	INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR
Address	:	Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur. 85111
Scope	:	**Specialized Agencies of the Regional Bodies for Performance Assessment and Development**

The above-mentioned organization has been assessed by SIS CERTIFICATION as certification body, and being proceed for issuing **INTEGRATION MANAGEMENT SYSTEM of ISMS ISO 27001:2022, Certificate by SISCERT (SIS CERTIFICATION).**

This letter is obtained only for notification to the 3rd party and valid maximum 3 (three) months from the date of this statement of conformity issued. **(July 05, 2024 – October 05, 2024).**

For further information in detail, please contact to Representative SISCERT Indonesia office by email msf.siscertindonesia@gmail.com , or phone no + 6281328206962.

Sincerely Yours,

Dr. Arfanda. Anugrah Siregar,ST .,M.Si
Rep. Head Official SISCERT Indonesia

SIS CERT.

We Do Not Sell, We Certify!

SURVEILLANCE

AUDIT REPORT AS PER ISO 37001:2016 (ABMS) & ISO /IEC 27001:2022 (ISMS)-IMS

SIS CERTIFICATIONS

Client's Name: INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR

Visit No.: Surveillance

Date of Opening meeting: 04.07.2024

Date of Closing Meeting: 05.07.2024

Applicable Standard(s): ISO 37001:2016 (ABMS) & ISO/IEC 27001:2022 (ISMS)

TABLE OF CONTENTS

SIS Certifications

Part-1: Executive Summary

Client Details

Client registration No.	
Client Name	**INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR**
Address	**Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur. 85111**
Other Location(site)	
Primary contact	**Stefanus F. Halla, S.T., M.M, CGCAE**
Contact No.	
Email	
Communication contact	**Feronika Naatonis, S.T. M.Eng., QRMP**
Contact No.	
Email	
Scope of the organization	**Specialized Agencies of the Regional Bodies for Performance Assessment and Development**
Categories	
Total No. of Employees	
Total No. of Students	
Audit Duration(s)	**02 MD**
SIS Audit team*	**Lead Auditor: Ivar Kusradi D. ST., M. Eng**
Audit Criteria*	**To audit Within ISO 19011, The Manuals, Procedures, documents, Records, Implementation of the system as per the specific Requirements of ISO 37001:2016 & ISO/IEC 27001:2022.**
Audit Objectives	**To** • **Ensure Audit internal processes and management.** • **Review actions on previous nonconformities.** • **Review complaints handling.** • **Assess management system effectiveness.** • **Monitor progress for continual improvement activities.** • **Ensure ongoing operational control.** • **Review any changes.** • **Check use of marks and references to certification.**
Any Deviation from the Audit Plan?	**If yes: - Specify Reason**
Any significant issues impacting on the audit program?	**If yes: - Please specify**
Date(s) of Audit	**04-05.07.2024**
Type of Previous Audit/Date(s)	
Type of Audit	**Individual** ☐ **Combined** ☐ **Joint** ☐ **Integrated** ■
Location	**On Site** ☐ **Permanent Site** ■ **Temporary Site** ☐ **Off site** ☐ **Remote audit** ☐

**The audit team leader shall conduct audit as per SIS Auditor Guidelines of conducting audits, ref: Document no: SIS/AG/01, Issue no: 02, rev02, effective date: 02.05.2019*

** The audit shall be conducted on a sample-based approach. One or more samples shall be drawn from the set of process/products and the audit findings shall be based on the results of the audit of the sample(s).*

*****Opening/Closing Meetings:*** *Opening and closing meetings were performed in accordance with SIS Form Ref no. sis/op.cl/F/01. The objective of the audit was to confirm that the management system had been established and implemented in accordance with the requirements of the audit standard.*

Audit Result

The organization has implemented all the requirements in ISO 37001:2016 (ABMS) & ISO 27001:2022 (ISMS), so it can be ensured that all stakeholders understand, especially the changes to the requirements in the 2022 version of ISMS. Top management is very enthusiastic in carrying out the audit and is supported by all staff employees within ITDA NTT Province, the results of field verification prove the commitment and consistency of the organization. Implementation and ongoing evaluation of each department within the scope of certification contributes to each requirement including ANNEX (SoA).

Summary of the Audit

I.	Any significant changes in the management system as compared to the previous audit? Yes
II.	Any Unresolved issues from the previous audit? No
III.	Previous N.C /Observations Closed? Yes
IV.	Improvement/changes in the Management system as compared to the previous audit. Yes
V.	Conclusion stating the Scope of certification is appropriate to the system being followed. Yes
VI.	Confirmation that audits objectives have been fulfilled? Yes
VII.	_**10**___**Minor**/_0___Major Nonconformance/__**3**__ **Observation**/_____OFI identified in the audit, details of Non-Conformance are detailed in NCCAP (As Attached Along). Please respond by using NCCAP form and include the root cause analysis with systemic corrective action. The inappropriate action on the NCCAP may result in the non-acceptance by the concerned auditor.

The auditors therefore recommend:

☒	***Continuation of Certificate*** ☐***The ABMS & ISMS complies with the requirements of the reference standard:*** *Congratulations, on the basis of the above summary, Lead Auditor is pleased to put forward a recommendation for Continuation of Certificate* ☐ ***The ABMS & ISMS complies with the requirements of the reference standard with exception of Observations:*** *Congratulations, Lead Auditor is pleased to put forward a recommendation for continuation of the Certification of the Organization upon off-site verification of root cause & Corrective action plan of all issues, the Action Plan for the observations need to be submitted with 15 days from the audit. If all Observations are not closed within 15 days due to any Reason a proper justification is required on the Email & the same needed to be closed within 30 days from the Audit, if not done the grading of the finding is to be changed to higher degree as applicable.* ☒ ***The ABMS & ISMS complies with the requirements of the reference standard with exception of minor NC:*** *Congratulations, Lead Auditor is pleased to put forward a recommendation for continuation of the Certification of the Organization upon off-site verification of closure of all issues, the NC closure need to be submitted along with the Corrective Action Plan with 15 days from the audit and objective evidence within the 60 days from the date of audit. If all non-conformances are not closed within 60 days, a full reassessment may be conducted.*
☐	***Refusal of the Certification*** ☐ ***Evidence of major nonconformities:*** *Organization is not recommended for Continuation of Certification. A follow-up assessment will be scheduled to allow for on-site verification and closure of all issues within 60 days from the date of Surveillance audit. If all non-conformances are not closed within 60 days, a full reassessment may be conducted.* *Or any other relevant reason*_____
☐	***Follow Up audit*** ☐***Not Recommended:*** *Organization is not recommended for continuation of certification, a Surveillance audit will be required. To progress your application for registration, please respond to each non-conformance, with a plan showing proposed actions, timescales and responsibilities for resolution. The organization should consider the root cause of the non-conformance and the potential for related issues in other parts of your system.*
☐	*Other (if any):*
	Next Surveillance/Re-Certification Audit (MM/YYYY): July 2025

SIS Certifications

Audit finding

S.No.	Clause No.	Requirements	Statement of nonconformance:	Category (Major N.C/ Minor N.C/ Observations/ OFI	For client use only		Reviewed by/Date *(For SIS office use only)*
					Corrective action and Root Cause Analysis	Evidence of Closure (Documents /Photograph/Visit)	
ISMS ISO 27001:2022							
1.	6.2	Sasaran Kinerja SMKI	Terlihat penetapan Sasaran Kinerja penerapan SMKI ISO 27001:2022 telah dilaksanakan sebagaimana semestinya, akan tetapi beberapa point berikut perlu di evaluasi antara lain: a. Point 7 berkaitan dengan penilaian kinerja penyedia pihak luar/vendor (barang atau jasa), jelaskan lebih detail aktivitas apa yang menjadi tolok ukur keberhasilan berkaitan dengan keamanan informasi, agar tidak missed-lead dengan ISO 9001 & ISO 37001 b. Point 9 perlu di-evaluasi, apakah masih relevan dengan SMKI terkait pelaksanaan WFH/ work from home untuk saat ini c. Pastikan penetapan sasaran kinerja berbasis pada SMKI versi 2022	**Minor - 01**			
2.	A. 5.24; A. 5.27	Manajemen Insiden	Perlu dilakukan evaluasi pada SOP Kejadian/ insiden (belum ada nomor SOP & nama pejabat/ sub koordinator substansi/ pastikan disesuaikan dengan nomenklatur saat ini), antara lain: a. Pastikan bahwa aktivitas analisis terdokumentasi mengenai **"Akar Masalah atau Penyebab"** terjadinya insiden harus dideskripsikan dalam laporan tindaklanjut (RTL),	**Observasi - 01**			

			b. Pastikan bahwa dilakukan review terhadap **"Efektifitas Mitigasi Risiko"** yang ditetapkan saat ini, pastikan pada dokumen risiko insiden terkait telah teridentifikasi, jika belum maka lengkapi sebagai risiko, pada dokumen risiko SMKI				
3.	A. 5.12	Klasifikasi data/informasi	Berdasarakan hasil audit, belum ada bukti berkaitan dengan penetapam klasifikasi data/ informasi maka ITDA Prov. NTT, maka: a. Pimpinan perlu menetapkan kebijakan klasifikasi data/ informasi dan, b. Tim SMKI dan masing-masing stake-holder internal ITDA melakukan identifikasi klasifikasi informasi/ data berdasarkan pemetaan risiko keamanan informasi yang telah ditetapkan, misalkan kategori data publikasi, data risiko rendah, data risiko menengah, data sensitive, data rahasia dan data sangat rahasia	**Minor - 02**			
4.	A.5.22; A. 7.7;	Monitoring, review and change management of supplier services; Clear desk and clear screen; physical entry	Beberapa aktivitas berikut yang telah ditetapkan dalam Nota Dinas No. IP.771/09/2024 tertanggal 26 Juni 2024; akan tetapi belum optimal terlaksana secara konsisten dan bukti terdokumentasi antara lain: a. Point 2, melaksanakan secara random pengujian password per 3 bulan terhadap computer pengolah data terutama di area ANEV dan computer para-auditor di setiap IRBAN; A.7.2 b. Point 7, terkait pemusnahan kertas yang berisikan informasi masih belum optimal dan masih terlihat belum dihancurkan ketika masuk kotak sampah, pastikan adanya "Warning Board/ pengingat" disemua area dekat printer; A.7.7	**Minor - 03**			

			c. Point 10, lokasi tempat services perangkat keras (perlu menetapkan penyedia jasa eksternal untuk services semua perangkat keras ketika harus diperbaiki, dengan melakukan seleksi dan uji kepatutan keamanan informasi); A.5.22				
5	A.5.11; A.6.5	Responsibilities after termination; Return of assets	Pertimbangkan agar organisasi melengkapi sarana untuk memastikan bahwa: a. Jika ada pegawai ASN/ Non ASN yang dipindahkan/ rotasi, purna-tugas dilengkapi dengan exit form yang berkaitan dengan penggunaan asset informasi/ data yang melekat pada yang bersangkutan, buatkan daftar pertanyaan yang menyangkut sarana utama, pendukung dan sistem akses yang bersangkutan talah diserahterimakan kepada tim SMKI dan di-approval oleh pimpinan; b. Jika ada pihak exernal yang diberikan akses sementara seperti Mahasiswa, Pihak External yang sedang melakukan	**Observasi - 02**			
6.	A.8.25	Secure development life cycle	Pastikan bahwa organisasi memiliki sistem **Prosedure Terdokumentasi (SOP) terkait membuat aplikasi baru atau pengembanagan aplikasi yang ada**, seperti Aplikasi E-Simple, pastikan bahwa setiap aplikasi baru yang mengolah data, telah terdaftar sebagai asset pengolah informasi/ data, resmi dan diketahui/ approval oleh pimpinan, diuji cobakan, baru di-release secara resmi.	**Minor - 04**			
7.	A.5.23	Information security for use of cloud services	Organisasi harus menetapkan Sistem prosedur terdokumentasi/ SOP terkait sistem penyimpanan data berbasis pada CLOUD, menentukan dan mengelola konsep keamanan informasi terkait layanan cloud yang mengatur keamanan informasi organisasi	**Minor - 05**			

8.	A.5.32	Intellectual property rights	Organisasi harus menetapkan prosedur terdokumentasi (SOP) berkaitan dengan perlindungan Hak Cipta/ karya inteletual property untuk melindungi segala informasi dan atau data yang diciptakan oleh pegawai/ staff organisasi	**Minor - 06**			
9.	A.7.13	Equipment Maintenance	Peralatan yang mendukung dan melidungi sarana perangkat pengolah sistem informasi harus dipelihara dengan benar untuk memastikan ketersediaan, integritas dan kerahasiaan informasi (SOP No. SMKI.09.2022, pasal 10), misalkan Pemeliharaan Penangkal Petir / Belum ada bukti laporan pemeliharan berdasarakan Nota Dinas No. IP.771/57/2024 (penagamanan sarpras dan pengolah asset informasi dari gangguan faktor cuaca)	**Minor - 07**			
10.	A.7.14	Secure disposal or re-use of equipment	Pastikan bahwa, team SMKI, harus melakukan **evaluasi secara periodik (SIDAK-pengujian konsistensi penerapan sistem),** selain Internal Audit, sesuai dengan prosedur terdokumentasi/ SOP yang berkaitan penerapan SMKI (kategori evaluasi termasuk memastikan **EFEKTIF atau tidaknya dalam implementasinya** dan ditetapkan dalam bukti laporan terdokumentasi secara periodik, seperti: Nota Dinas No. IP.771/09/2024 Tentang pelaksanaan SMKI ISO 27001:2022 i.e., Pengujian Penerapan Pembuatan Password (huruf besar, kecil, angka, symbol), Penerapan clean-desk, Penerapan firewall, dllnya dijadikan “checklist – verification/ SIDAK”	**Minor - 08**			
11		Physical security perimeters; Management of technical	Beberapa point aktivitas berikut ini Ruang arsip/ ANEV, perlu diperbaiki dan ditindaklanjuti antara lain: a. Ketersediaan Kunci lemari arsip **filling-cabinet**, belum ditemukan selama audit, filling-cabinet	**Minor - 09**			

		vulnerabilities; Physical security monitoring; Storage media; Secure disposal or re-use of equipment; Use of privileged utility programs	menyimpan arsip Hardcopy kategori **RIKSUS** dan lainnya, A.7.1 b. Pastikan bahwa CCTV tidak mudah dipindah-pindahkan arah dan posisinya, **(fixed placement), A.7.4** c. Pastikan pengelolaan sampah kertas hasil printout yang tidak terpakai, telah di hancurkan, sebelum masuk tempat sampah, dan jika diperlukan dilengkapi dengan Tata-cara/ warning-board di setiap area tempat sampah kertas (pisahkan antara sampah kertas yg berisi informasi, dan sampah lainnya/ organic, 7.7 d. Pastikan penggunaan email resmi/ formal yang ditetapkan sebagai sarana distribusi data/ informasi (terlihat penggunaan email terindikasi belum optimal/ karena distribusi data masih menggunakan flash-disk, yang berpotensi tidak **secure**), pastikan untuk kirim-terima/komunikasi data, terutama untuk LHP dengan berbagai klasifikasinya (sensitive/ sangat rahasia) tidak menggunakan flash-disk, A.8.8 e. Komputer penyimpanan data LHP dalam format PDF memiliki **KERENTANAN TINGGI,** karena beberapa point saat audit berlangsung: ○ Belum aktif screen-saver saat audit, A.7.7 ○ Perpindahan data/ distribusi data melalui flash-disk, A.8.8 ○ Belum dilakukan pengujian password secara berkala, A.7.14 ○ Pola penyimpanan (Tata-Folder) pada computer harus diatur terutama untuk data-data soft-file, Pemeriksaan Khusus,				

			○ Pemeriksaan Tertentu, dan seterusnya yang memiliki kategori klasifikasi sensitive, A.7.10 ○ Belum ditentukan siapa saja PIC yang memiliki otorisasi mengolah data dn jaringan Komputer ANEV (misalkan penyimpan data LHP dalam format Soft-File, siapa saja yang diberi akses privilege), A.8.18				
SMAP ISO 37001:2016							
12.	8.2.C	Uji tuntas/ due diligence	Perlu dipertimbangkan bahwa dalam penetapan auditor/ APIP yang telah dilengkapi dengan pakta integritas dan uji kepatutan, pada parameter/ kriteria dilengkapi lagi dengan beberapa point berkaitan dengan integritas, kapabilitas, kompetensi, pengalaman, hubungan kekerabatan, latar pendidikan dan penilaian kinerja (pertimbangkan dengan melengkapi sistem score/ quantitative)	**Observasi – 01**			
13.	4.5	Penilaian risiko penyuapan	Terlihat bahwa pemetaaan risiko i.e., risk register / ITDA) tahun 2024 disetiap bagian menggunakan Formulir Identifikasi Risiko kemudian diteruskan dalam dokumen Identifkasi Titik Rawan Praktik Gratifikasi dan ditetapkan Mitigasi Risiko Terhadap hasil Identifikasi Titik Rawan Gratifikasi (personal /PIC), akan tetapi belum lengkap dan perlu dilengkapi bahwa antara risk register yang ditetapkan juga sama dan teridentifikasi pada Mitigasi risiko yang ditetapkan untuk disemua lokasi yang ada pada dokumen risk register.	**Minor – 01**			

Previous audit finding Status-Closure

S.NO	Details of finding(s) raised and client action	Outcome (Closed or escalated)
	Yes, all of previous finding has been closed	closed

Description of the organization

An organization tasked with providing guidance and supervision to all regional organizational units periodically and as an assistant to the governor of the NTT regional head in order to prevent inappropriate activities and violations of established rules and regulations

Scope of certification

Scope of certification	Specialized Agencies of the Regional Bodies for Performance Assessment and Development
Requirements of standard to be excluded from scope:	N/A
Reason for exclusion and Justification:	N/A

Part-2: Audit Programme-Cycle

Stage of Audit	Stage-1	Stage-2	S1	S2	S3	S4	S5	Re-certification
Visit Due date (MM/YY) *	2022	2022	2023	2024				2025
Section of Standard	• The next visit shall be in Red, and Audited Section Mark Cross-(**X**)							
Context of the organization *(All Parts 4.1 to 4.4)*	X	X	X	X				X
Leadership *(All Parts 5.1 to 5.3)*	X	X	X	X				X
Planning *(All Parts 6.1 to 6.3)*	X	X	X	X				X
Supports *(All Parts 7.1 to 7.5)*	X	X	X	X				X
Operation *(All Parts 8.1 to 8.3)*	X	X	X	X				X
Performance evaluation *(All Parts 9.1 to 9.3)*	X	X	X	X				X
Improvement *(All Parts 10.1 to 10.2)*	X	X	X	X				X
Annex A: Reference control objectives and controls	X	X	X	X				X
Use of Logos (SIS & Accreditation)								

*S-Surveillance

*This audit Programme is to be prepared by the Lead Auditor at the completion of the Stage 2 audit or the Recertification audit. It should be replicated in all subsequent surveillance visit reports.

*Site visits are to be included in the Programme with a clear indication as to the processes intended to be sampled.

*Audit trails will be developed based upon identified risk throughout the audit and as such timings and content may be subject to change. Where the client operates shifts, the activities that take place during shift working shall be considered when developing the audit Programme.

Unit No. 514, 5th Floor,Vipul Business Park, Sohna Road, Sector – 48, Gurgaon-122018, Haryana, India.

LINK DOKUMEN NCCAP ITDA ISO 27001:2022

INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR TAHUN 2024

https://drive.google.com/drive/folders/1bNbB2zy-I8T0tFnEQE5krf7cvTN1n7AL?usp=sharing

LINK DOKUMEN TINDAK LANJUT ITDA ISO 27001:2022

INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR TAHUN 2024

https://drive.google.com/drive/folders/11jSdvTEkG6JRFRl5sLqIoOF6mku6o5aM?usp=sharing

CERTIFICATE OF REGISTRATION

SIS CERT.™
We Do Not Sell, We Certify!

This Certificate has been awarded to

INSPEKTORAT DAERAH PROVINSI NUSA TENGGARA TIMUR

Jl. Palapa No.06, Oebobo, Kec. Oebobo, Kota Kupang, Nusa Tenggara Timur. 85111, Indonesia

In recognition of the organization's Management System which complies with

ISO/IEC 27001:2022

Information Security, Cybersecurity and Privacy Protection — Information Security Management System

The scope of activities covered by this certificate is defined below

SUPERVISION AND GUIDANCE FOR THE IMPLEMENTATION OF GOVERNMENT AFFAIRS IN PROVINCIAL AREAS AND REGENCY/ CITY AREAS

SoA Details :- ITDA/SoA/Ver.02/Rev.01 (27001:2022) Dated on 20 May 2024

SYNDICATE OF INTERNATIONAL SYSTEM CERTIFICATIONS

Certificate Number: **SIS410722I108**
Date of Initial Registration: **26.07.2022**
Latest Date of Issue: **17.08.2024**
Expiry Date: **25.07.2025**
Re-certification Due on: **26.06.2025**

Managing Director

SIS CERTIFICATIONS PVT. LTD.

IAS ACCREDITED Management Systems Certification Body MSCB-131

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

Note: The certificates is the property of SIS Certifications & the Validity of the Certificate is subject to the successful completion of Surveillance Audit on or before the due date. (In case Surveillance Audit is not allowed to be conducted, this Certificate shall be suspended and must be returned immediately upon request.)

Certified Organization is responsible for maintaining the compliance of the relevant standard rules. Any significant changes in the scope of the certification or standard referred above render this certificate invalid

Corporate office- **SIS Certifications Pvt. Ltd.**
Unit No. 514, 5th Floor, Vipul Business Park, Sector-48, Sohna Road, Gurgaon-122018, Haryana, India.
International Subcontractor Key Locations: **Qatar, Egypt, Italy, Canada & USA.**
Email us:- support@siscertifications.com, Call /Whatsapp: +91-9643073391
The status of this certificate can be verified on "https://siscertifications.com
Web:- www.siscertifications.com

Issue No.: **03**