CHECKLIST AUDIT INTERNAL ISO 27001:2022

Lokasi / Departemen : _____	Tanggal Audit : _____	Auditor : _____
Scope SMKI : _____	Periode Audit : _____	**Halaman 1 dari 5**

KLAUSUL 4 & 5 — KONTEKS ORGANISASI & KEPEMIMPINAN

No	Item Pemeriksaan	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agt	Sep	Okt	Nov	Des
1	Isu internal & eksternal relevan sudah teridentifikasi dan terdokumentasi												
2	Pihak berkepentingan (stakeholder) & kebutuhannya sudah dipetakan												
3	Ruang lingkup SMKI ditetapkan secara tertulis (batasan fisik & logis)												
4	Komitmen manajemen puncak terhadap SMKI terbukti nyata												
5	Kebijakan keamanan informasi ditetapkan & dikomunikasikan ke semua karyawan												
6	Peran, tanggung jawab & wewenang keamanan informasi terdefinisi jelas												
	Paraf Auditor & Tanggal												

Keterangan : **v** Conform / OK **X** Non-Conform / Butuh Perbaikan **O** Observasi / Peluang Perbaikan (OFI)

Jika ditemukan NC, segera catat di Lembar Temuan dan laporkan ke Management Representative / CISO.

CHECKLIST AUDIT INTERNAL ISO 27001:2022

Lokasi / Departemen : _____	Tanggal Audit : _____	Auditor : _____
Scope SMKI : _____	Periode Audit : _____	**Halaman 2 dari 5**

KLAUSUL 6 & 7 — PERENCANAAN & DUKUNGAN

No	Item Pemeriksaan	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agt	Sep	Okt	Nov	Des
1	Penilaian risiko menggunakan metodologi yang terdokumentasi & konsisten												
2	Rencana Perlakuan Risiko (RTP) disusun & disetujui manajemen												
3	Statement of Applicability (SoA) mencakup 93 kontrol Annex A												
4	Tujuan keamanan informasi ditetapkan secara SMART												
5	Sumber daya (anggaran, SDM, infrastruktur) memadai tersedia												
6	Kompetensi personel keamanan informasi terdokumentasi & tersertifikasi												
7	Program pelatihan & kesadaran keamanan dilaksanakan min. 1x/tahun												
8	Dokumen & rekaman dikendalikan (versi, akses, penyimpanan, disposal)												
	Paraf Auditor & Tanggal												

Keterangan : **v** Conform / OK **X** Non-Conform / Butuh Perbaikan **O** Observasi / Peluang Perbaikan (OFI)

Jika ditemukan NC, segera catat di Lembar Temuan dan laporkan ke Management Representative / CISO.

CHECKLIST AUDIT INTERNAL ISO 27001:2022

Lokasi / Departemen : _____	Tanggal Audit : _____	Auditor : _____
Scope SMKI : _____	Periode Audit : _____	**Halaman 3 dari 5**

KLAUSUL 8, 9 & 10 — OPERASIONAL, EVALUASI & PERBAIKAN

No	Item Pemeriksaan	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agt	Sep	Okt	Nov	Des
1	Proses operasional SMKI direncanakan, diimplementasikan & dikendalikan												
2	Penilaian risiko diulang berkala / saat ada perubahan signifikan												
3	Perlakuan risiko dilaksanakan sesuai RTP yang disetujui												
4	Monitoring & pengukuran efektivitas SMKI dilakukan & direkam												
5	Program audit internal berjalan sesuai jadwal; auditor independen												
6	Management Review dilakukan min. 1x/tahun; dihadiri manajemen puncak												
7	Setiap nonconformity ditangani dengan tindakan korektif terstruktur												
8	Root Cause Analysis dilakukan; efektivitas koreksi dievaluasi												
	Paraf Auditor & Tanggal												

Keterangan : **v** Conform / OK **X** Non-Conform / Butuh Perbaikan **O** Observasi / Peluang Perbaikan (OFI)

Jika ditemukan NC, segera catat di Lembar Temuan dan laporkan ke Management Representative / CISO.

CHECKLIST AUDIT INTERNAL ISO 27001:2022

Lokasi / Departemen : _____	Tanggal Audit : _____	Auditor : _____
Scope SMKI : _____	Periode Audit : _____	**Halaman 4 dari 5**

ANNEX A — KONTROL ORGANISASI & MANUSIA (Kritis)

No	Item Pemeriksaan	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agt	Sep	Okt	Nov	Des
1	Kebijakan keamanan informasi & turunannya (sub-policies) tersedia												
2	Pemisahan tugas (Segregation of Duties) diterapkan pada proses kritis												
3	Manajemen kapasitas TI dipantau untuk menghindari gangguan layanan												
4	Keamanan rantai pasok: vendor kritikal dinilai & persyaratan dikontrakkan												
5	Onboarding/offboarding karyawan mencakup aspek keamanan informasi												
6	Insiden keamanan dilaporkan & ditangani via prosedur formal												
7	Background check dilakukan untuk posisi dengan akses tinggi												
8	Prosedur disiplin tersedia & diterapkan untuk pelanggaran keamanan												
	Paraf Auditor & Tanggal												

Keterangan : **v** Conform / OK **X** Non-Conform / Butuh Perbaikan **O** Observasi / Peluang Perbaikan (OFI)

Jika ditemukan NC, segera catat di Lembar Temuan dan laporkan ke Management Representative / CISO.

CHECKLIST AUDIT INTERNAL ISO 27001:2022

Lokasi / Departemen : _____	Tanggal Audit : _____	Auditor : _____
Scope SMKI : _____	Periode Audit : _____	**Halaman 5 dari 5**

ANNEX A — KONTROL FISIK & TEKNOLOGI (Kritis)

No	Item Pemeriksaan	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agt	Sep	Okt	Nov	Des
1	Perimeter keamanan fisik (kunci, badge, CCTV) berfungsi baik												
2	Akses ruang server hanya untuk personel berwenang; log akses tersedia												
3	Kebijakan clean desk & clear screen diterapkan & dipatuhi												
4	Perlindungan ancaman fisik tersedia: UPS, fire suppression, raised floor												
5	Manajemen kerentanan: scan berkala, patching, verifikasi remediation												
6	Kontrol akses RBAC (least privilege) diterapkan & direviu berkala												
7	Multi-Factor Authentication (MFA) aktif di sistem & remote access kritikal												
8	Log aktivitas diaktifkan, dilindungi dari modifikasi & direviu berkala												
9	Backup data kritikal diuji pemulihannya & disimpan di lokasi terpisah												
10	Enkripsi diterapkan: data at rest & in transit pada aset sensitif												
	Paraf Auditor & Tanggal												

Keterangan : **v** Conform / OK **X** Non-Conform / Butuh Perbaikan **O** Observasi / Peluang Perbaikan (OFI)

Jika ditemukan NC, segera catat di Lembar Temuan dan laporkan ke Management Representative / CISO.