



**ASOSIASI LAYANAN URUN DANA INDONESIA
(ALUDI)**

**PERKUMPULAN SECURITIES CROWDFUNDING
INDONESIA**

Kantorkuu coworking & office space, Citywalk Sudirman lantai 2,
Jl.KH.Mas Mansyur no.121 RT 10/RW 11, Kel.Karet Tengsin Kec.
Tanah Abang, Jakarta Pusat 10220.

Memahami Manfaat Sertifikasi ISO 27001 Bagi Penyelenggara Sistem Elektronik

Era digitalisasi saat ini membuat sebuah peradaban ‘seolah-olah berpindah’ pada sebuah jaringan internet dan perangkat. Mulai dari pagi hingga malam hari, kegiatan manusia pada saat ini mayoritas merupakan kegiatan yang mengharuskan dirinya untuk terhubung dalam jaringan internet. Di Indonesia tercatat pada tahun 2022 setidaknya 210 juta masyarakat telah menjadi pengguna internet.¹ Berdasarkan perkembangan dari tahun ke tahunnya, diproyeksikan jumlah ini akan terus meningkat pada tahun-tahun selanjutnya.² Demikian, hal ini menjadi bukti bahwa era digital saat ini semakin nyata dan setiap orang harus bersiap-siap mengantisipasinya.

Berbicara mengenai perkembangan dunia digital, baru-baru ini pemerintah Indonesia telah mengeluarkan suatu peraturan yang mewajibkan para pelaku usaha yang menyelenggarakan suatu kegiatan sistem elektronik dan mengelola data pribadi masyarakat untuk melindungi data yang dikelolanya, yakni Undang-Undang 27 Tahun 2022 tentang Perlindungan Data Pribadi (“UU No. 27/2022”). Bagi pihak yang melanggarnya, terdapat sejumlah ganjaran sanksi yang dapat diterima seperti mulai dari ancaman kurungan penjara, apabila pelakunya orang perseorangan, atau pemberhentian kegiatan usaha, apabila pelakunya korporasi. Adapun diketahui bahwa undang-undang ini terbit atas respon pemerintah terhadap banyaknya isu kebocoran data pribadi di Indonesia yang merugikan masyarakat.³ Demikian menjadi penting untuk mengantisipasi terjadinya kebocoran data tersebut. Selain untuk mencegah kerugian bagi pemilik data, namun juga untuk menghindari peneraan sanksi kepada pelaku usaha.

Dalam konteks ini, sejatinya terdapat beberapa upaya preventif yang dapat dilakukan perusahaan. Salah satu upayanya adalah dengan melakukan Sertifikasi ISO 27001:2013. ISO 27001:2013 ini adalah sebuah dokumen standar Sistem Manajemen Keamanan Informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh

¹ CNN Indonesia, “Data Terbaru! Berapa Pengguna Internet Indonesia 2022?,” <https://www.cnbcindonesia.com/tech/20220609153306-37-345740/data-terbaru-berapa-pengguna-internet-indonesia-2022>, diakses 21 Desember 2022.

² *Ibid.*

³ FIA UI, “UU Perlindungan Data Pribadi dan Tantangan Implementasinya,” <https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/>, diakses 21 Desember 2022.



ASOSIASI LAYANAN URUN DANA INDONESIA
(ALUDI)

PERKUMPULAN SECURITIES CROWDFUNDING
INDONESIA

Kantorkuu coworking & office space, Citywalk Sudirman lantai 2,
Jl.KH.Mas Mansyur no.121 RT 10/RW 11, Kel.Karet Tengsin Kec.
Tanah Abang, Jakarta Pusat 10220.

sebuah organisasi atau *enterprise* dalam usaha mengimplementasikan suatu konsep keamanan informasi.⁴ Tidak hanya itu, dokumen ini juga merupakan salah satu standar yang bertujuan dalam menggambarkan sistem manajemen keamanan informasi. Hal ini diperoleh dari dilakukannya audit aspek sistem manajemen keamanan informasi.⁵ Tujuannya tidak lain adalah untuk menjamin adanya perlindungan informasi. Selain itu, dengan memperoleh sertifikasi ISO 27001 ini sejatinya dapat membawa banyak keuntungan bagi suatu perusahaan. Adapun keuntungan yang dimaksud seperti diantaranya adalah:⁶

1. Meyakinkan klien dan pemangku kepentingan tentang bagaimana perusahaan mengelola risiko.
2. Memungkinkan pertukaran informasi yang aman.
3. Membantu perusahaan untuk mematuhi persyaratan hukum.
4. Membantu memberi perusahaan keunggulan kompetitif.
5. Mempromosikan kepuasan pelanggan yang meningkatkan retensi klien.
6. Membantu menjaga konsistensi dalam pengiriman produk atau layanan perusahaan.
7. Membantu mengelola dan meminimalkan paparan risiko.
8. Membantu membangun budaya keamanan.

Secara lebih lanjut, untuk memperoleh dokumen ISO 27001:2013 akan terdapat 7 (tujuh) tahapan yaitu:⁷

1. *Gap Analysis*

Sebelum menerapkan ISO 27001 pada organisasi/perusahaan, penting untuk dilakukan *Gap Analysis* terlebih dulu. Ini penting guna mengetahui kondisi nyata perusahaan untuk kemudian dianalisis apakah dengan kondisi tersebut sudah bisa menerapkan manajemen keamanan informasi atau tidak.

2. **Kajian Risiko**

Mengingat apa pun yang dilakukan pasti memiliki risiko, penting bagi perusahaan untuk melakukan analisis atau kajian terhadap hal ini. Dengan harapan,

⁴ IT Governance Indonesia, "ISO 27001 Adalah Ikon Standarisasi Manajemen Keamanan Informasi," <https://itgid.org/iso-27001-adalah/>, diakses 21 Desember 2022.

⁵ *Ibid.*

⁶ Eduparx, "4 Alasan Utama Perusahaan Anda Perlu Menerapkan Standar ISO 27001," <https://eduparx.id/blog/insight/4-alasan-standar-iso-27001-penting/>, diakses 21 Desember 2022.

⁷ Mutu Institute, "Cara Mendapatkan Sertifikat ISO 27001:2013 Terbaru," <https://mutuinstitute.com/post/cara-mendapatkan-sertifikat-iso-27001/>, diakses 21 Desember 2022.

perusahaan bisa mengetahui berbagai potensi risiko yang bisa muncul dan mengancam aset informasi. Hal ini dilakukan untuk kemudian dirumuskan langkah pencegahan atau mitigasi guna melindungi aset informasi tersebut.

3. Penyusunan Dokumen

Dalam hal ini, baik tahap *gap analysis* maupun kajian risiko harus perusahaan dokumentasikan dengan baik. Mengingat hasil dari kedua tahap tersebut akan dibutuhkan untuk tahap perencanaan, implementasi, hingga evaluasi.

4. Internal Audit

Setelah implementasi berjalan, tim bisa melakukan evaluasi kinerja atau audit internal. Tujuannya adalah untuk melakukan *internal assessment* guna mengetahui sejauh mana progres dari penerapan manajemen keamanan informasi tersebut. Jika progresnya telah menunjukkan hasil positif, maka proses bisa langsung dilanjutkan pada tahap audit sertifikasi. Sebaliknya, jika masih ditemukan masalah atau hambatan, tim harus menganalisis serta merumuskan langkah perbaikan untuk menanganinya.

5. Persiapan Audit Sertifikasi

Sebelum melakukan proses audit sertifikasi, perusahaan juga perlu melakukan persiapan, baik secara teknis, dokumentasi, ataupun dari segi mental para tim yang akan menghadapi para auditor. Dalam hal ini, lakukan persiapan sebaik-baiknya agar proses audit bisa berjalan lancar dan perusahaan bisa mendapatkan sertifikat ISO 27001:2013.

6. Audit Sertifikasi

Dalam realitanya, organisasi atau perusahaan yang mengajukan sertifikat ISO 27001:2013 harus melalui proses audit oleh badan sertifikasi terlebih dulu. Pada tahap ini, tim auditor akan memeriksa apakah perusahaan telah mampu menerapkan semua klausa yang ada pada ISO 27001 atau tidak, serta bagaimana efektivitasnya.

Jika misal masih ada kesalahan atau penyimpangan, tim auditor akan mencatat dan menunjukkannya pada manajemen perusahaan. Untuk nantinya, diberikan waktu perbaikan sesuai dengan tingkat penyimpangan. Di sini, tim manajemen perusahaan bisa melakukan berbagai langkah atau tindakan korektif untuk memperbaiki



**ASOSIASI LAYANAN URUN DANA INDONESIA
(ALUDI)**

**PERKUMPULAN SECURITIES CROWDFUNDING
INDONESIA**

Kantorkuu coworking & office space, Citywalk Sudirman lantai 2,
Jl.KH.Mas Mansyur no.121 RT 10/RW 11, Kel.Karet Tengsin Kec.
Tanah Abang, Jakarta Pusat 10220.

kesalahan tersebut. Jika telah selesai dan pihak auditor telah setuju, baru sertifikat akan diterbitkan.

7. Implementasi ISO 27001

Setelah memiliki sertifikat ISO 27001 bukan berarti tugas suatu perusahaan telah selesai. Perusahaan harus tetap konsisten dalam menerapkan standar manajemen keamanan informasi, mengingat ini adalah sistem berkelanjutan dimana juga membutuhkan kerja sama dari semua pihak internal perusahaan.

Penulis : **Adhityo Adya**



**ASOSIASI LAYANAN URUN DANA INDONESIA
(ALUDI)**

**PERKUMPULAN SECURITIES CROWDFUNDING
INDONESIA**

Kantorkuu coworking & office space, Citywalk Sudirman lantai 2,
Jl.KH.Mas Mansyur no.121 RT 10/RW 11, Kel.Karet Tengsin Kec.
Tanah Abang, Jakarta Pusat 10220.

DAFTAR PUSTAKA

- CNN Indonesia. “Data Terbaru! Berapa Pengguna Internet Indonesia 2022?.”
<https://www.cnbcindonesia.com/tech/20220609153306-37-345740/data-terbaru-berapa-pengguna-internet-indonesia-2022>. Diakses 21 Desember 2022
- FIA UI. “UU Perlindungan Data Pribadi dan Tantangan Implementasinya.”
<https://fia.ui.ac.id/uu-perlindungan-data-pribadi-dan-tantangan-implementasinya/>
Diakses 21 Desember 2022.
- IT Governance Indonesia. “ISO 27001 Adalah Ikon Standarisasi Manajemen Keamanan Informasi.” <https://itgid.org/iso-27001-adalah/>. Diakses 21 Desember 2022.
- Eduparx. “4 Alasan Utama Perusahaan Anda Perlu Menerapkan Standar ISO 27001.”
<https://eduparx.id/blog/insight/4-alasan-standar-iso-27001-penting/>. Diakses 21 Desember 2022.
- Mutu Institute. “Cara Mendapatkan Sertifikat ISO 27001:2013 Terbaru.”
<https://mutuinstitute.com/post/cara-mendapatkan-sertifikat-iso-27001/>. Diakses 21 Desember 2022.