Institut Informatika & Bisnis
DARMAJAYA
Yayasan Alfian Husin

3

Standar dan Kerangka Kerja Keamanan Informasi

ISO 27000 *Information Security Management System*

Keamanan Informasi

Pengelolaan keamanan informasi yang baik dan efektif adalah di mana suatu organisasi memperhitungkan seluruh proses baik operasional dan organisasional termasuk pihak yang terkait dengan keamanan informasi.

ISO 27000 *Information Security Management System*

ISO dan IEC (*International Electrotechnical Commission*) bersepakat dalam mengembangkan standar keamanan informasi seri 2700x.

1. *ISO 27000:2009 - Information Security Management System - Overview and vocabulary*
2. *ISO 27001:2005 - Information Security Management System - Requirements*
3. *ISO 27002:2005 – Code of Practise for Information Security Management System*
4. *ISO 27003:2010 – Information Security Management System Implementation Guidance*
5. *ISO 27004:2009 – Information Security Management System Measurement*
6. *ISO 27005:2008 – Information Security Risk Management System*
7. *ISO 27006:2011 – Requirements for Bodles Providing Audit and Certification of Informastion Security Management System*

ISO 27000
Information Security Management System

8. *ISO 27007:2011 – Guidelines for Information Security Management System Auditting (Focused on the Management System).*
9. *ISO 27008:2011 – Guidance for Auditors on ISMS Controls (Focused on Information Security Controls)*
10. *ISO 27010:2011 – Information Technology – Security Techniques –Information Security Management for Inter-sector and Inter-Organizational Communications*
11. *ISO 27011:2008 – Information Security Management Guidelines for Telecommunication Organizational based on ISO/IEC 27002.*
12. *ISO 27013:2015 – Guideline on the Integrated implmentation of ISO/IEC 20000-1 and ISI/IEC 27001*
13. *ISO 27014 : Information Security Governance Framework*
14. *ISO 27015 : Information Security Management Guidelines for the Finance and Insurances Sectors*
15. *ISO 27016 – Information Security Management – Organiozational Economics [DRAFT]*
16. *ISO 27017 – Security in Cloud Computing [DRAFT]*

ISO 27000
Information Security Management System

17. *ISO 27018 – Code of Practice for Data Protection Controls for Public Cloud Computing Services [DRAFT]*
18. *ISO 27019 – Information Security Management Guidelines based on ISO 27002 for Process Control Systems Specific to the Energy Industry [DRAFT]*
19. *ISO 27031:2011 – Guidelines for Information and Communication Technology Readiness for Business Cntinuity.*
20. *ISO 27032:2012 – Guidelines for Cyber Security*
21. *ISO 27033:2008 – IT Network Security, a Multi-part Standard based on ISO/IEC 18028:2006*
22. *ISO 27034:2011 – Guidelines for Application Security (part 1 published rest in DRAFT)*
23. *ISO 27033:2011 – Information Security Incident Management*
24. *ISO 27036 – Information Security for Suppler Realtionship [DRAFT]*
25. *ISO 27037:2012 – Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.*

ISO 27000
Information Security Management System

26. *ISO 27038 – Specification for Digital Redaction [DRAFT]*
27. *ISO 27038 – Selection, Development and Operations of Intrusion Detection (and preventation) [DRAFT]*
28. *ISO 27040 – Storage Security [DRAFT]*
29. *ISO 27041 – Guidelines for the Analysis and Interpretation of Digital Evidence [DRAFT]*
30. *ISO 27042 – Guidelines for the Analysis and Interpretation of Digital Evidence [DRAFT]*
31. *ISO 27043 – Digital evidence investigation Principles and Process [DRAFT]*
32. *ISO 27799:2008 – Information Security Management in Health using ISO/IEC 27002.*

Standar ISO 13335

Standar ISO 13335 merupakan standar yang digunakan untuk *Management of Information and Communications Technology Security*. Standar ini berisi arahan umum untuk menginisiasi dan mengimplementasikan proses manajemen keamanan teknologi inforkan masi. Standar ini hanya menyediakan instruksi untuk mengelola keamanan teknologi informasi, bukan sebagai solusi keamanannya.

ISO 27001

ISO 27001 (*Information Technology - Security Techniques – Information Security Management Systems Requirement Spesification*) merupakan standar internasional pertama yang bisa di sertifikasi untuk manajemen keamanan informasi. Standar ini berisi rekomendasi umum untuk menjalankan dan meningkatkan dokumentasi manajemen keamana sistem informasi dengan mempertimbangkan berbagai risiko.

ISO 27002

Sebelumnya ISO 27002 dikenal dengan nama ISO 17799:2005 (*Information Technology - Code of Practice for Information Security Management*) memiliki tujuan untuk menentukan kerangka kerja manajemen keamanan informasi. Standar ini fokus terhadap langkah-langkah yang diperlukan untuk membangun fungsionalitas sistem manajemen keamanan dan mengimplementasikannya ke dalam organisasi. rekomendasi dari standar ini khususnya untuk tingkat manajemen dan tidak banyak memiliki informasi teknis yang spesifik.

ISO 27005

ISO 27005 (*Information Security Risk Management*) merupakan standar yang berisi rekomendasi umum untuk manajemen risiko keamanan informasi. Standar ini digunakan untuk mendukung implementasi ISO 27001.

ISO 27006

ISO 27006 (*Information Technology - Security Techniques – Requirements for The Accreditation of Bodies Providing Certification of Information Security Management Systems*) berisi penjelasan dari persyaratan yang dibutuhkan untuk mengakreditasi sertifikasi ISMS dan detail prosesnya secara spesifik.

International Organization for Standarization (ISO) 27001:2009

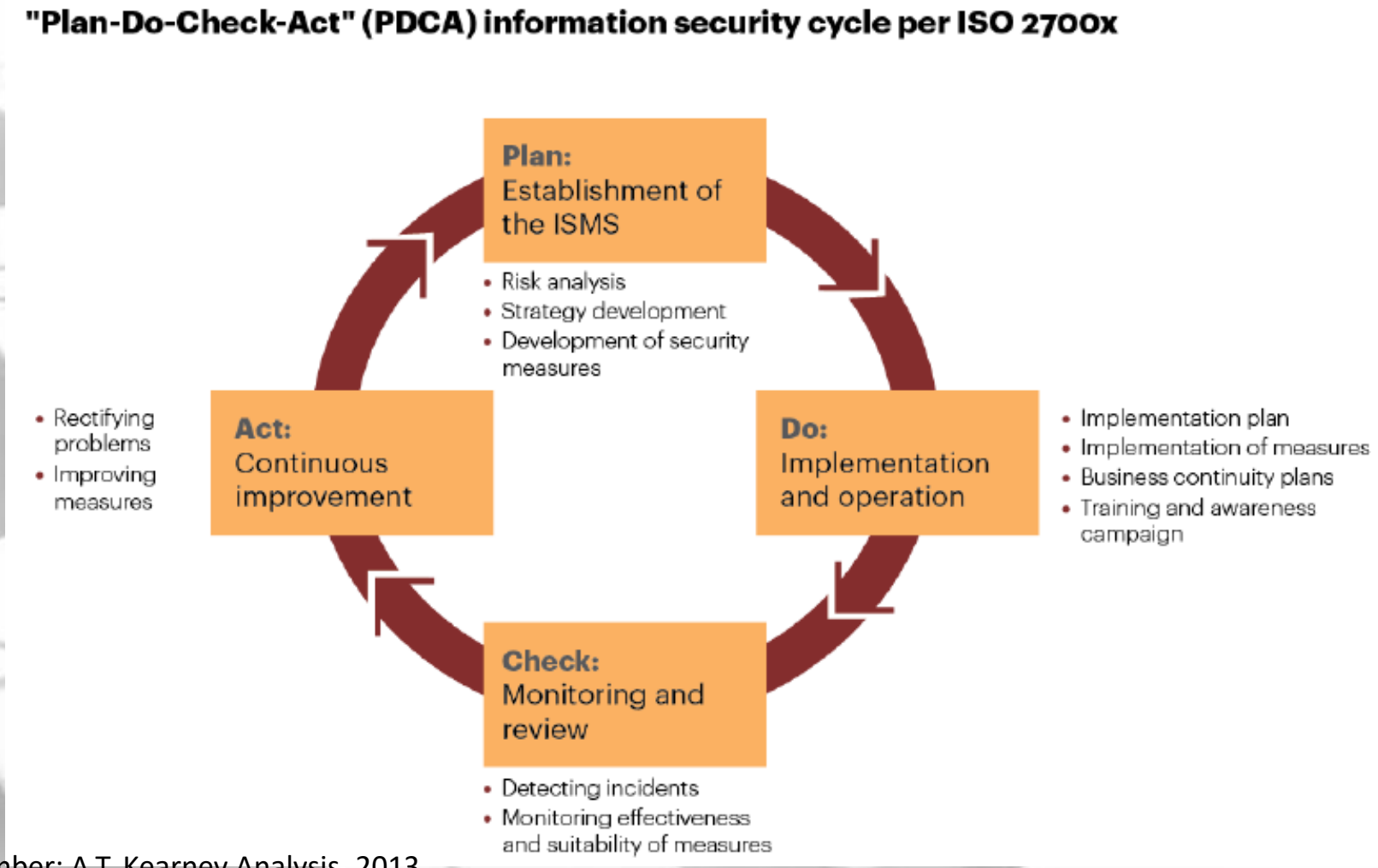
- ISO merupakan badan standar internasional yang mengembangkan dan mempublikasikan sebuah sistem manajemen untuk menilai mutu organisasi.
- Badan Standarisasi Nasional (BSN) mempublikasikan Standar Nasional Indonesia (SNI) ISO/IEC 27001:2009 yang diadopsi dari ISO/IEC 27001:2005 dalam rangka mendukung sistem keamanan informasi bagi lembaga penyelenggara pelayanan publik.
- Dalam menerapkan **sistem manajemen keamanan informasi (SMKI)**, ISO 27001 mendefinisikan 11 klausul, 39 objektif kontrol, dan 133 kontrol (Kemenpora, 2012)

Kelompok Kebutuhan Pengendalian Keamanan

Proses Perancangan Manajemen Keamanan Informasi

- Tujuan Standar ISO 27001:2009 adalah sebagai acuan untuk pembangunan, pengoperasian, pengimplementasian, peninjauan, pengawasan, pemeliharaan dan perbaikan sistem manajemen keamanan informasi.
- ISO 27001 menggunakan siklus *Plan-Do-Check-Act* (PDCA)

Siklus PDCA pada ISO 27001



Sumber: A.T. Kearney Analysis, 2013

Siklus PDCA pada ISO 27001

Plan

- Pada tahap ini dilakukan penetapan tujuan, aturan, proses, dan prosedur yang sesuai untuk mengelola risiko dan meningkatkan keamanan informasi. Hal ini bertujuan agar dapat memberikan hasil sesuai dengan tujuan dan kebijakan organisasi.

Do

- Selanjutnya dilakukan penerapan dan jalannya aturan, kontrol, kebijakan, proses dan prosedur **sistem manajemen keamanan informasi (SMKI)** yang sudah dipilih di tahap sebelumnya.

Siklus PDCA pada ISO 27001

Check

- Tahap selanjutnya dilakukan penilaian, pengawasan, dan peninjauan penerapan dari SMKI dan jika memungkinkan bila dilakukan pengukuran kinerja proses terhadap kebijakan SMKI, dan hasilnya akan dilaporkan ke pihak manajemen untuk ditinjau lebih lanjut.

Act

- Pada tahap terakhir dilakukan langkah-langkah perbaikan dan pencegahan yang diambil berdasarkan hasil dari audit internal SMKI dan *management review* atau informasi lainnya yang berhubungan untuk mencapai perbaikan SMKI secara berkelanjutan.

Perancangan SMKI di Perusahaan

1. Menentukan ruang lingkup dan batasan dari SMKI
2. Menentukan kebijakan SMKI yang berhubungan dengan bisnis, organisasi, aser, teknologi, dan lokasi.
3. Menentukan pendekatan penilaian risiko organisasi.
4. Mengindentifikasi risiko aset, ancaman, kerawanan, dan dampak dari hilangnya kerahasiaan, ketersediaan, dan integritas yang mungkin terjadi terhadap aset.
5. Menganalisa dan mengevaluasi risiko, dan mengestimasi level risiko.
6. Mengidentifikasi dan mengevaluasi pilihan untuk perlakuan terhadap risiko.
7. Memilih kontrol dan kontrol objektif untukperlakuan terhadap risiko.
8. Mendapatkan persetujuan dari pihak manajemen terhadap perlakuan risiko.
9. Mendapatkan otoritas manajemen untuk menerapkan dan menjalankanSMKI.
10. Menyiapkan *Statement of Applicability,*

Penerapan dan Menjalankan SMKI

1. Merumuskan perencanaan tindak lanjut risiko untuk menentukan tindakan yang sesuai bagi.
2. Menerapkan perencanaan tindak lanjut risiko untuk mencapai kontrol objektif.
3. Menerapkan kontrol yang sudah dipilih untuk mencapai objektif kontrol.
4. Menentukan cara mengukur efektifitas kontrol yang sudah dipilih dan menentukan juga apakah dapat digunakan untuk menilai efektivitas kontrol.
5. Menerapkan program pelatihan dan kesadaran terhadap keamanan informasi.
6. Mengelola operasional SMKI.
7. Mengelola sumber daya SMKI.
8. Menerapkan langkah-langkah dan kontrol lainnya yang bisa menemukan dan merespon jika terjadi kejadian yang berhubungan dengan keamanan sistem.

Pengawasan dan Peninjauan SMKI

1. Menjalankan langkah-langkah pengawasan dan peninjauan serta kontrol lainnya.
2. Melakukan tinjauan secara berkala terhadap efektivitas SMKI dengan melihat hasil dari audit keamanan, hasil dari efektivitas pengukuran, insiden, saran, dan masukan dari berbagai pihak yang berkaitan.
3. Mengukur efektivitas kontrol untuk memastikan kebutuhan keamanan telah terpenuhi.
4. Meninjau penilaian risiko pada jangka waktu tertentu dan sisa risiko serta level risiko yang sudah diidentifikasi.
5. Menjalankan audit internal SMKI sesuai dengan jangka waktu yang telah ditetapkan.
6. Meninjau pihak manajemen terhadap SMKI untuk memastikan ruang lingkup terpenuhi dan proses perbaikan SMKI dapat dikenali.
7. Melakukan perbaharuan rencana dengan mempertimbangkan hal-hal yang ditemui dalam kegiatan pengawasan dan peninjauam SMKI.
8. Mendokumentasikan semua kegiatan dan kejadian yang bisa berdampak pada efektivitas dan kinerja SMKI.

Menjaga dan Meningkatkan SMKI

Tahap terakhir dari siklus PDCA

1. Menerapkan perbaikan yang teridentifikasi di SMKI.
2. Mengambil tindakan perbaikan dan pencegahan. Kemudian menerapkan pelajaran yang didapat dari pengalaman di dalam maupun luar organisasi yang terkait dengan keamanan.
3. Mengkomunikasikan tindakan dan perbaikan kepada semua pihak yang terkait.
4. Memastikan perbaikan tersebut sudah memenuhi sasaran yang diharapkan.

Domain dan Kontrol Objektif SNI ISO 27001:2009

Sumber: SNI ISO 27001:2009

Ref. Annex A	Domain & Kontrol Objektif
A.5	Kebijakan keamanan
A5.1	Kebijakan keamanan informasi
A.6	Organisasi keamanan informasi
A6.1	Organisasi internal
A6.2	Pihak eksternal
A.7	Pengelolaan aset
A7.1	Tanggung jawab terhadap aset
A7.2	Klasifikasi informasi
A.8	Keamanan sumberdaya manusia
A8.1	Belum dipekerjakan
A8.2	Selama bekerja
A8.3	Pengakhiran atau perubahan pekerjaan

Domain dan Kontrol Objektif SNI ISO 27001:2009

Sumber: SNI ISO 27001:2009

Ref. Annex A	Domain & Kontrol Objektif
A.9	**Keamanan fisik dan lingkungan**
A9.1	Area yang aman
A9.2	Keamanan peralatan
A.10	**Manajemen komunikasi dan informasi**
A10.1	Prosedur operasional dan tanggung jawab
A10.2	Manajemen pelayanan jasa pihak ketiga
A10.3	Perencanaan dan keberterimaan sistem
A10.4	Perlindungan terhadap malicious dan mobile code
A10.5	Back-up
A10.6	Manajemen keamanan jaringan
A10.7	Penanganan media
A10.8	Pertukaran informasi
A10.9	Layanan electronic commerce
A10.10	Pemantauan

Domain dan Kontrol Objektif SNI ISO 27001:2009

Sumber: SNI ISO 27001:2009

Ref. Annex A	Domain & Kontrol Objektif
A.11	**Pengendalian akses**
A11.1	Persyaratan bisnis untuk pengendalian akses
A11.2	Manajemen akses pengguna
A11.3	Tanggung jawab pengguna
A11.4	Pengendalian akses jaringan
A11.5	Pengendalian akses sistem informasi
A11.6	Pengendalian akses aplikasi dan informasi
A11.7	Mobile computing dan kerja jarak jauh (teleworking)
A.12	**Akuisisi, pengembangan dan pemeliharaan sistem informasi**
A12.1	Persyaratan keamanan dari sistem informasi
A12.2	Pengelolaan yang benar dalam aplikas
A12.3	Pengendalian dengan cara kriptografi

Domain dan Kontrol Objektif SNI ISO 27001:2009

Sumber: SNI ISO 27001:2009

Ref. Annex A	Domain & Kontrol Objektif
A12.4	Keamanan system files
A12.5	Keamanan dalam proses pengembangan dan pendukung
A12.6	Manajemen kerawanan teknis
A13	**Manajemen insiden keamanan informasi**
A13.1	Pelaporan kejadian dan kelemahan keamanan informasi
A13.2	Manajemen insiden keamanan informasi dan perbaikan
A.14	**Manajemen keberlanjutan bisnis (Business continuity management)**
A14.1	Aspek keamanan informasi dari manajemen keberlanjutan Bisnis
A.15	**Kesesuaian**
A15.1	Sesuaian dengan persyaratan hukum
A15.2	Pemenuhan terhadap kebijakan keamanan dan standar, dan pemenuhan teknis
A15.3	Pertimbangan audit sistem informasi

11 Klausul Kontrol Keamanan

1. **Kebijakan keamanan**: komitmen Manajemen dan dukungan untuk kebijakan keamanan informasi ditujukan dalam domain ini.
2. **Organisasi keamanan informasi:** koordinasi dan pengelolaan usaha informasi organisasi keamanan secara keseluruhan adalah rinci dalam domain ini. Tanggung jawab keamanan informasi didefinisikan dalam domain ini.
3. **Pengelolaan aset:** semua aset kritis dan sensitif didefinisikan dalam domain.
4. **Keamanan sumberdaya manusia**: domain ini membahas kesadaran pengguna dan pelatihan. Pengguna kesadaran dan pelatihan dapat mengurangi risiko pencurian, penipuan, dan kesalahan.
5. **Keamanan fisik dan lingkungan**: domain ini membatasi akses ke fasilitas ke petugas yang berwenang. Selain itu, alamat domain membatasi jumlah kerusakan yang terjadi pada bangunan fisik dan informasi organisasi.

11 Klausul Kontrol Keamanan

6. **Manajemen komunikasi dan operasi**: domain ini membahas risiko kegagalan dan konsekuensi yang dihasilkan. Hal ini dicapai dengan memastikan penggunaan yang tepat dan aman dari fasilitas pengolahan informasi.
7. **Pengendalian akses**: domain ini memastikan akses ke sistem masing-masing dan informasi dibatasi untuk petugas yang berwenang. Deteksi kegiatan yang tidak sah juga dibahas dalam domain ini.
8. **Akuisisi, pengembangan dan pemeliharaan sistem informasi**: domain ini membahas kerugian dan penyalahgunaan informasi dalam aplikasi yang digunakan dalam perusahaan.
9. **Manajemen insiden keamanan informasi**: peristiwa dan kelemahan keamanan harus dilaporkan. Domain ini membahas definisi tanggung jawab dan prosedur pengelolaan insiden keamanan dan perbaikan, serta mengumpulkan bukti-bukti untuk insiden keamanan.
10. **Manajemen keberlanjutan bisnis:** domain ini membahas kemampuan organisasi untuk secara cepat merespon setiap gangguan sistem bisnis penting. Gangguan sistem ini dapat disebabkan oleh kegagalan *hardware*, insiden, dan bencana alami.
11. **Kesesuaian:** domain ini membahas kepatuhan hukum oleh bisnis. Selain itu, domain ini memastikan bahwa tujuan yang ditetapkan oleh manajemen tingkat atas sedang diikuti dan bertemu.