Keamanan SPBE
Konsep Dasar Audit Keamanan Informasi: Pedoman Audit SistemManajemen (ISO 19011:2018)

Bersama BSSN Negara Aman dan Sejahtera

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

BADAN SIBER DAN SANDI NEGARA

PENGANTAR ISO 19011

- Pengertian Audit
- Tipe Audit
- Istilah-istilah

Audit Keamanan Informasi

- ISO 27000 (2018) & 19011– Glossary

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled

Audit Sebuah proses yang sistematik, independen dan terdokumentasi untuk mencari bukti-bukti audit dan mengevaluasi bukti-bukti tsb secara objective (tidak subjective) untuk menentukan sejauh mana kriteria audit telah dipenuhi.

www.assignmentdesk.co.uk

What is an Audit?

An audit is an investigation conducted by an independent party into a company's financial report. The aim of an audit is to provide assurance (different from a guarantee) that the financial statements are true and fair according to the relevant financial reporting framework.

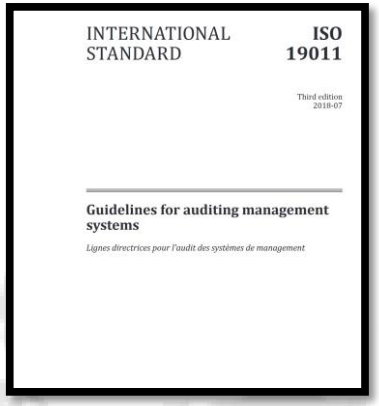
BADAN SIBER DAN SANDI NEGARA

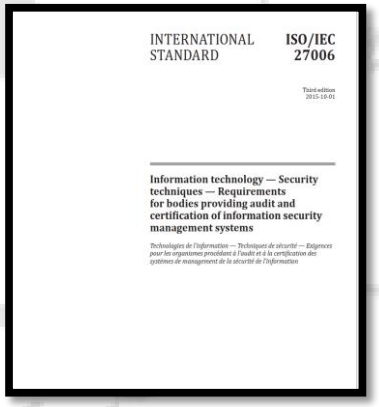
BADAN SIBER DAN SANDI NEGARA

ISO TERKAIT GUIDELINE AUDIT

- ISO 17021 : 2015 - Conformity assessment — Requirements for bodies providing audit and certification of management systems
- ISO 19011 : 2018 - Guidelines for auditing management systems
- ISO 27006:2015 - Information technology — Security. techniques Requirements. for bodies providing audit and certification of information security management systems


INTERNATIONAL STANDARD
ISO/IEC 17021-1
First edition 2015-06-15
NG PURPOSE ONLY
Conformity assessment — Requirements for bodies providing audit and certification of management systems —
Part 1: Requirements
Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management — Partie 1: Exigences


INTERNATIONAL STANDARD
ISO 19011
Third edition 2018-07
Guidelines for auditing management systems
Lignes directrices pour l'audit des systèmes de management


INTERNATIONAL STANDARD
ISO/IEC 27006
Third edition 2015-10-01
Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

BADAN SIBER DAN SANDI NEGARA

Tujuan Audit

1. Memeriksa kesesuaian antara standar, regulasi, prosedur dengan kondisi penerapan di lapangan
2. Menjamin konsistensi dalam penerapan di lapangan
3. Mencari poin-poin untuk peningkatan dan perkembangan terhadap kondisi di lapangan
4. Mematuhi peraturan terkait pelaksanaan audit
5. Sebagai pemenuhan permintaan dari pelanggan atau pasar

BADAN SIBER DAN SANDI NEGARA

Type Audit

Audit Pihak Pertama

Audit Pihak Kedua

Auditor Pihak Ketiga

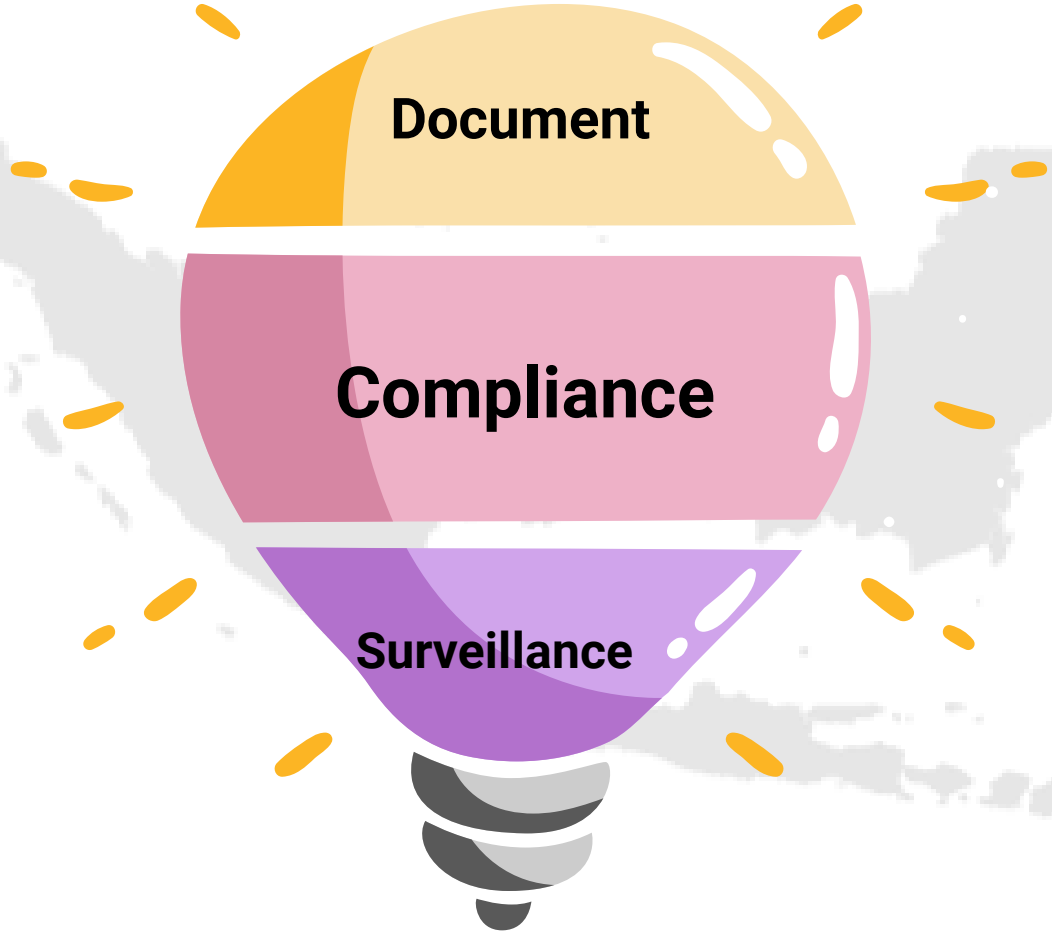
Audit pihak 1 - **Audit Internal**, adalah proses audit yang dilaksanakan oleh organisasi sendiri untuk keperluan evaluasi internal. Audit internal ini sebaiknya menggunakan auditor yang merupakan pegawai organisasi tersebut.

Audit pihak 2 - **Audit Pemasok**, adalah bentuk audit yang dilakukan oleh pelanggan terhadap pemasoknya untuk memastikan kinerja pemasok dalam memberikan produk atau jasa sesuai dengan ketentuan pelanggan.

Audit Pihak 3 - **Audit Eksternal**, adalah bentuk audit yang dilakukan dalam proses sertifikasi. Dilaksanakan oleh lembaga yang independent/lembaga sertifikasi yang tidak memiliki kepentingan atas kinerja instansi yang diaudit.

BADAN SIBER DAN SANDI NEGARA

Tipe Audit Lainnya



1. Review terhadap dokumen(prosedur, kebijakan dan petunjuk) yang ada di organisasi tujuannya menentukan kesesuaian dokeumen dengan standar

2. Menentukan implementasi standar pada sistem sudah sesuai kriteria kesesuaian

3. Menentukan penerapan standar yg berjalan secara berkelanjutan sesuai dengan persyaratan .

BATANG TUBUH
ISO 19011_1

- Standard Panduan Audit
- Prinsip Audit
- Kompetensi Auditor

Prinsip Audit

ISO 19011: 2018 - Guidelines for auditing management systems

- Integritas
- Jujur
- Profesional
- Menjaga kerahasiaan
- Independen
- Pendekatan berdasarkan bukti
- Pendekatan berbasis risiko

BADAN SIBER DAN SANDI NEGARA

Audit Kaminfo Component

Audit Criteria

set of policies, procedures or requirements used as a reference against which audit evidence is compared

Audit Evidence

records, statements of fact or other information which are relevant to the audit criteria (3.2) and verifiable

Audit Scope

extent and boundaries of an audit

Audit Findings

results of the evaluation of the collected audit evidence (3.3) against audit criteria

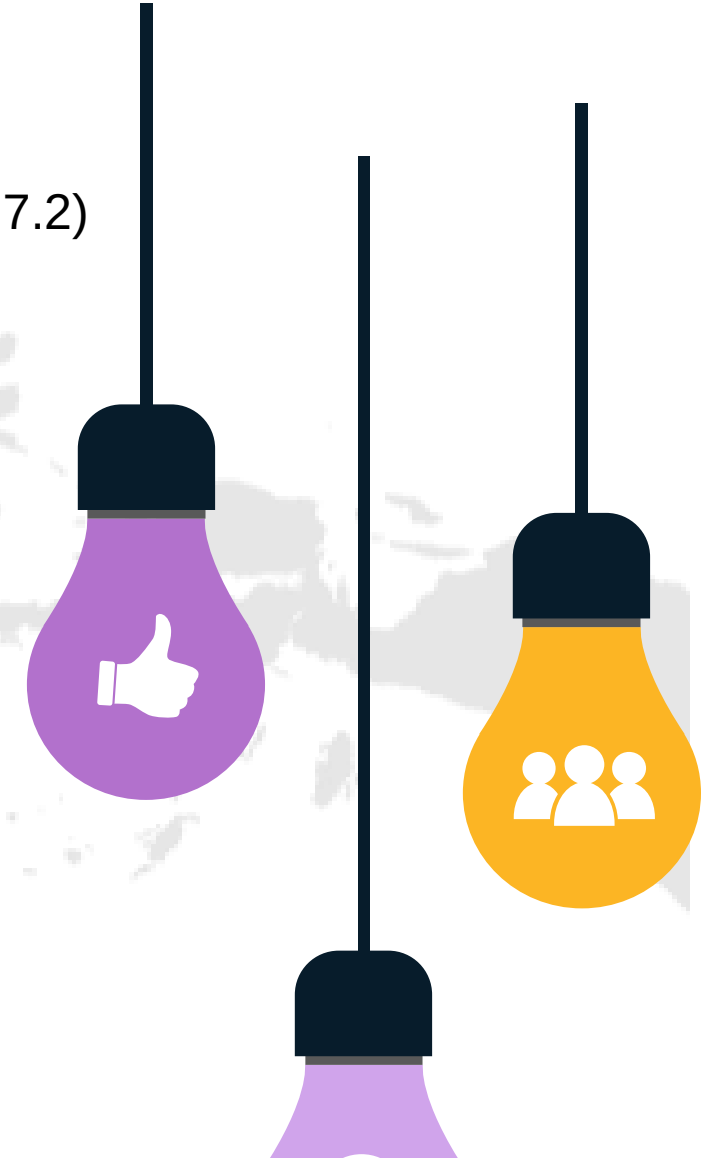
Audit Kaminfo Methode

Metode Evaluasi	Obyektif	Contoh
Tinjauan catatan	Untuk verifikasi latar belakang auditor	Analisis catatan pendidikan, pelatihan, pekerjaan dan pengalaman audit
Umpan balik positif dan negatif	Untuk memberikan informasi mengenai kinerja auditor	Survei, kuesioner, referensi pribadi, pengakuan, keluhan, evaluasi kinerja, masukan kolega
Wawancara	Untuk evaluasi atribut personal dan ketrampilan berkomunikasi, untuk verifikasi informasi dan uji pengetahuan dan untuk memperoleh informasi tambahan	Tatap muka dan wawancara melalui telepon
Observasi	Untuk evaluasi atribut personal dan kemampuan untuk aplikasi pengetahuan dan keahlian	Role-play, witnessed audit, kinerja dalam pekerjaan
Ujian	Untuk evaluasi atribut personal dan pengetahuan dan keahlian dan aplikasinya	Oral dan ujian tertulis, tes psychometric
Tinjauan pasca audit	Untuk menyediakan informasi dimana observasi langsung tidak mungkin atau kurang sesuai	Tinjauan laporan audit dan diskusi dengan klien audit, auditee, kolega, dan dengan auditor

Kompetensi Auditor

Kompetensi yang harus dimiliki oleh auditor dalam ISO 19011: 2018 (klausul 7.2) meliputi personal behavior dan skill and knowladge.

- Pemahaman tentang standar sebagai kriteria audit
- Pemahaman kriteria audit lain mencakup regulasi terkait dan dokumen internal
- Pemahaman proses yang akan diaudit
- Pengalaman melakukan audit
- Kecakapan dalam berkomunikasi dan
- Berperilaku profesional (open minded).



BADAN SIBER DAN SANDI NEGARA

Kompetensi Auditor

Menjadi Auditor Sebaiknya

- Lebih bersahabat dan tidak tegang
- Pendengar yang baik dan lancar berkomunikasi (75% mendengar, 25% bertanya)
- Menunjukan minat yang tinggi
- Lebih objektif dan logis
- Berpandangan positif dan elalu menanggapi dengan baik → Hindari adu argumentasi
- Mudah bergaul dengan setiap tingkatan di organisasi
- Memiliki rasa ingin tahu yang tinggi
- Memahami teknologi dan hal-hal baru
- Hindari cari-cari kesalahan dan catat hal-hal yang baik juga
- Tepat waktu
- Periksa semua proses
- Hargai kerahasiaan organisasi
- Hindari membaca SOP/dokumen sendiri mintalah penjelasan.
- Audit sistem bukan individu

BATANG TUBUH ISO 19011_2

- Manajemen Program Audit
- Pelaksanaan Audit
- Pelaporan Audit

BADAN SIBER DAN SANDI NEGARA

Manajemen Program Audit – General

Program audit dapat dibuat untuk satu atau lebih standard sistem manajemen atau persyaratan lain, baik yang dilakukan terpisah atau bersama-sama (audit gabungan)

Untuk perusahaan yang memiliki beberapa objek lokasi audit atau ada fungsi-fungsi penting yang alihdayakan dan dikelola dibawah kepemimpinan organisasi lain maka diperlukan perhatian khusus pada **desain, perencanaan dan validasi** program audit

Manajemen Program Audit – General

Top Manajemen sebaiknya menunjuk seseorang yang bertanggung jawab untuk Manajemen Program Audit, dengan wewenang:

- Menetapkan, menerapkan, mengawasi, meninjaudan meningkatkan Program Audit
- Mengidentifikasi dan memastikan sumber daya yang diperlukan tersedia

Untuk organisasi yang lebih kecil atau kurang komplek maka program audit dapat disesuaikan dengan skalanya.

Dalam menyusun program audit memperhitungkan :

- Tujuan organisasi
- Isu eksternal dan internal yang relevan
- Kebutuhan dan harapan pihak berkepentingan yang relevan
- Persyaratan keamanan informasi dan kerahasiaan

BADAN SIBER DAN SANDI NEGARA

Pelaksanaan Audit

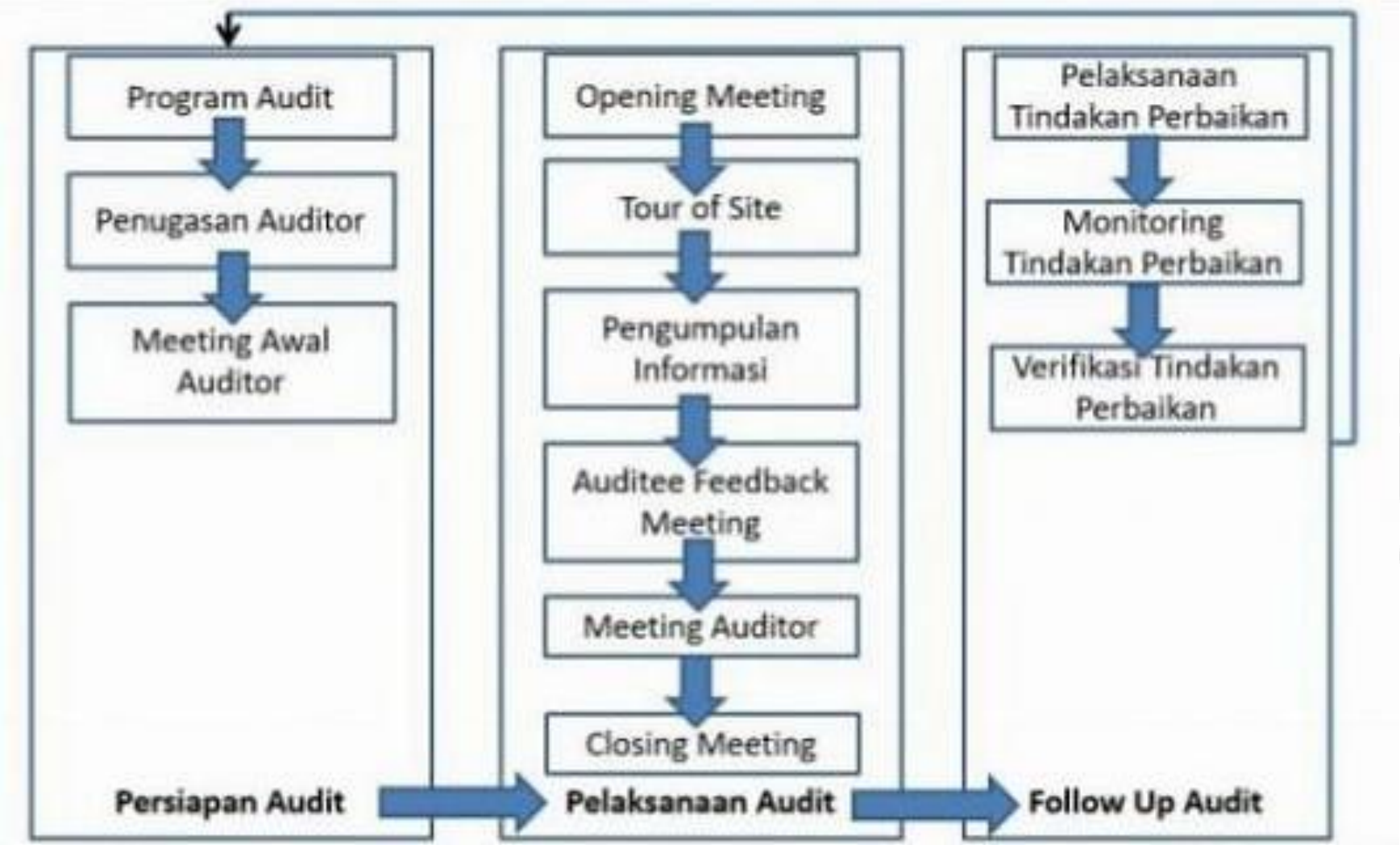
APPLICABLE AUDIT METHODS

Extent of involvement between the auditor and the auditee	Location of the auditor	
	On-site	Remote
Human interaction	Conducting interviews. Completing checklists and questionnaires with auditee participation. Conducting document review with auditee participation. Sampling.	Via interactive communication means: — conducting interviews; — observing work performed with remote guide; — completing checklists and questionnaires; — conducting document review with auditee participation.
No human interaction	Conducting document review (e.g. records, data analysis). Observation of work performed. Conducting on-site visit. Completing checklists. Sampling (e.g. products).	Conducting document review (e.g. records, data analysis). Observing work performed via surveillance means, considering social and legal requirements. Analysing data.
On-site audit activities are performed at the location of the auditee. Remote audit activities are performed at any place other than the location of the auditee, regardless of the distance. Interactive audit activities involve interaction between the auditee's personnel and the audit team. Non-interactive audit activities involve no human interaction with persons representing the auditee but do involve interaction with equipment, facilities and documentation.		

Alur Manajemen Program Audit

PLAN	• Membangun tujuan program audit • Menentukan dan mengevaluasi resiko dan peluang program audit • Membangun program audit
DO	Mengimplementasikan program audit
CHECK	Memonitor program audit
ACT	Menijau dan meningkatkan program audit

SIKLUS AUDIT



Persiapan Audit (PLAN)

- Persiapan Audit mencakup pembuatan **Program Audit** pada awal tahun oleh Koordinator Program Audit (Lead Auditor).
- Penugasan auditor melalui surat pengangkatan atau surat penugasan.
- Tim auditor melakukan meeting awal untuk menyusun **Audit Plan** dan membagi tugas audit internal diantara semua anggota tim auditor.
- Tim menyiapkan sampling plan dan mempelajari dokumen milik auditi dan laporan audit sebelumnya

Program Audit
Program audit mencakup informasi (PLAN)

- Tujuan untuk program audit
- Resiko dan peluang yang terkait dengan program audit dan tindakan untuk mengatasinya
- Ruang lingkup (luas, batas, lokasi) dari setiap audit dalam program audit
- Jadwal audit (nomor/durasi/frekuensi)
- Tipe audit (audit eksternal atau internal)
- Kriteria audit
- Metode audit yang akan digunakan
- Kriteria untuk menyeleksi anggota tim audit
- Informasi terdokumentasi yang relevan

Program audit harus dimonitor dan diukur secara berkelanjutan untuk memastikan tujuannya tercapai. Perlu dimonitor dikarenakan untuk mengidentifikasi kebutuhan untuk perubahan dan kemungkinan peluang untuk perbaikan.

Tujuan Audit (PLAN)

Tujuan Audit sebaiknya didasarkan pada beberapa pertimbangan sebagai berikut :

- Prioritas Manajemen
- Tujuan Komersial
- Karakteristik proses, produk, projek dan perubahan apapun yang terjadi padanya,
- Persyaratan Sistem Manajemen
- Persyaratan Perundangan dan Kontraktual
- Kebutuhan evaluasi vendor
- Persyaratan pelanggan dan Kebutuhan pihak – pihak yang berkepentingan
- Tingkat kinerja auditee terutama yang berkaitan dengan kegagalan ataupun keluhan pelanggan
- Risiko organisasi
- Tindak lanjut dari audit sebelumnya
- Tingkat kematangan dari sistem manajemen

Tanggung Jawab dan Peran (PLAN)

Manajer Program Audit bertanggung jawab untuk:

- Menetapkan **tujuan** dan **lingkup program audit**
- Mengindentifikasi dan mengevaluasi Risiko dari program audit
- Menetapkan tanggung jawab dan prosedur dan memastikan ketersediaan sumber daya
- Memastikan penerapan program audit
- Memastikan catatan terkait dengan program audit terpelihara
- Mengawasi, meninjau dan meningkatkan program audit

Penetapan Ruang Lingkup Audit (PLAN)

Manajer program audit sebaiknya menetapkan ruang lingkup dari program audit yang dapat bervariasi tergantung dari :

- *Ukuran organisasi*
- *Sifat organisasi*
- *Fungsi*
- *Kompleksitas dan tingkat kematangan organisasi*

Sebuah organisasi dapat memiliki audit program yang berisi satu jenis audit, tergantung dari jenis aktifitas dan struktur auditee.

Ruang Lingkup Program

Ruang lingkup Program Audit dipengaruhi oleh:

- Ruang lingkup,tujuan, waktu dan frekuensi audit
- Jumlah, kepentingan, kompleksitas, kesamaan sifat dan **lokasi, aktivitas** yang diaudit
- Faktor-faktor yang memepengaruhi keefektifan sistem manajemen
- **Standar**, peraturan dan persyaratan kontraktual serta kriteria lainnya yang berlaku
- Hasil dari audit (eksternal dan internal) dan tinjauan program audit sebelumnya
- Bahasa, budaya dan isu sosial
- Kepentingan dari pihak-pihak terkait (e.g. keluhan pelanggan dan ketidaktaatan terhadap peraturan)
- Perubahan yang mendasar dalam organisasi dan operasinya.
- Ketersediaan informasi dan teknologi informasi pendukung aktivitas audit (e.g. metode jarak jauh)
- Ketidaksesuaian yang terjadi baik dari internal ataupun eksternal (e.g. kegagalan produk dan bocornya keamanan informasi)

Identifikasi dan Evaluasi Risiko Program Audit

Terdapat Risiko yang bervariasi terkait dengan penetapan, implementasi, pemantauan dan peningkatan suatu program audit yang dapat mempengaruhi tujuan audit. Manajer program audit sebaiknya mempertimbangkan Risiko ini dalam mengembangkan program audit. Risiko-Risiko tersebut dapat terkait dengan

- Perencanaan (e.g. kegagalan dalam menetapkan tujuan audit dan ruang lingkup program audit)
- Sumber daya (e.g Kurangnya waktu pada pelaksanaan audit)
- Pemilihan tim audit (e.g. kompetensi yang tidak sesuai)
- Pelaksanaan audit (e.g. komunikasi yang tidak efektif)
- Pengendalian rekaman (e.g. kerusakan rekaman audit)
- Pengawasan, peninjauan dan peningkatan program audit (e.g. pengawasan ketidakefektifan program audit)

Menetapkan Prosedur Program Audit

Prosedur Program Audit sebaiknya ditetapkan **termasuk** :

- Membuat perencanaan dan jadwal Audit dengan mempertimbangkan Risiko program audit
- Memastikan keamanan informasi dan kerahasiaan
- Menjamin kompetensi auditor dan lead auditor
- Menyeleksi tim Audit, menetapkan tugas dan tanggung jawabnya
- Menentukan kompetensi Auditor dan Lead Auditor
- Melaksanakan audit termasuk penggunaan metode sampling yang sesuai
- Pelaksanaan tindak lanjut Audit, jika dapat dilaksanakan
- Pelaporan pencapaian program audit secara keseluruhan ke manajemen puncak
- Memelihara catatan Program Audit
- Mengawasi dan meninjau kinerja dan efektifitas Program Audit

BADAN SIBER DAN SANDI NEGARA

Menetapkan Sumber Daya

Pada saat mengidentifikasi sumberdaya program audit, kita sebaiknya mempertimbangkan:

- **Finansial** untuk mengembangkan, menerapkan, mengelola dan meningkatkan aktivitas audit
- Metode/ Teknik Audit
- Ketersediaan informasi dan teknologi komunikasi
- ketersediaan **auditor dan expert** (jika perlu) sesuai tujuan audit
- Lingkup program dan Risiko audit
- **Waktu perjalanan**, **akomodasi** dan kebutuhan lain

BADAN SIBER DAN SANDI NEGARA

Implementasi Program Audit

- **Mengkomunikasikan program audit** kepada pihak terkait
- **Menetapkan tujuan, lingkup dan kriteria untuk setiap audit**
- **Koordinasi dan penjadualan audit** dan aktivitas lain terkait dengan program audit
- Memastikan **pemilihan tim audit**
- Memastikan ketersediaan fasilitas yang dibutuhkan tim audit
- Meyakinkan **pelaksanaan audit** sesuai program audit
- Memastikan pengendalian **catatan** dari aktivitas audit

Pengawasan dan Peninjauan Program Audit (CEK)

Penerapan program audit sebaiknya **dimonitor dan ditinjau pada interval waktu** yang sesuai. Hasil tinjauan sebaiknya di laporkan kepada manajemen puncak. **Peninjauan program sebaiknya juga terhadap**:

- Tinjauan peningkatan kompetensi tim audit
- Laporan tinjauan efektivitas program audit

AUDIT IN ACTION

Pelaksanaan Audit (DO)

Pelaksanaan Audit dimulai dengan Opening Meeting, yang dilakukan bersama antara auditor dan auditi.

Jika diperlukan maka dilakukan Tour of Site untuk melihat kondisi lapangan.

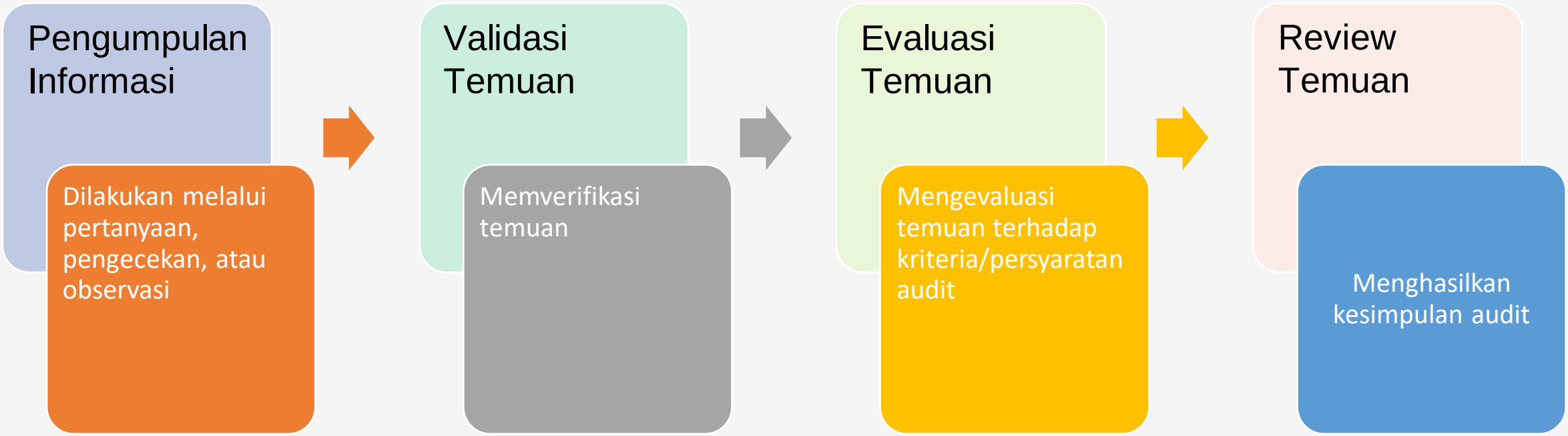
Pengumpulan informasi dapat dilakukan dengan wawancara atau review dokumen.

Diakhir hari audit, dilakukan Auditee Feedback Meeting untuk memastikan temuan yang didapat di hari itu dan juga membahas jadwal esok hari.

Sebelum closing meeting, auditor berkumpul untuk membahas semua temuan dan membuat kesimpulan audit.

Penyusunan Laporan Audit.

Proses Audit



STAGE 1 AUDIT

Stage 1

Purpose – to confirm that company's ISMS policy, manual and procedures meet the minimum requirements of the standard.

Activities

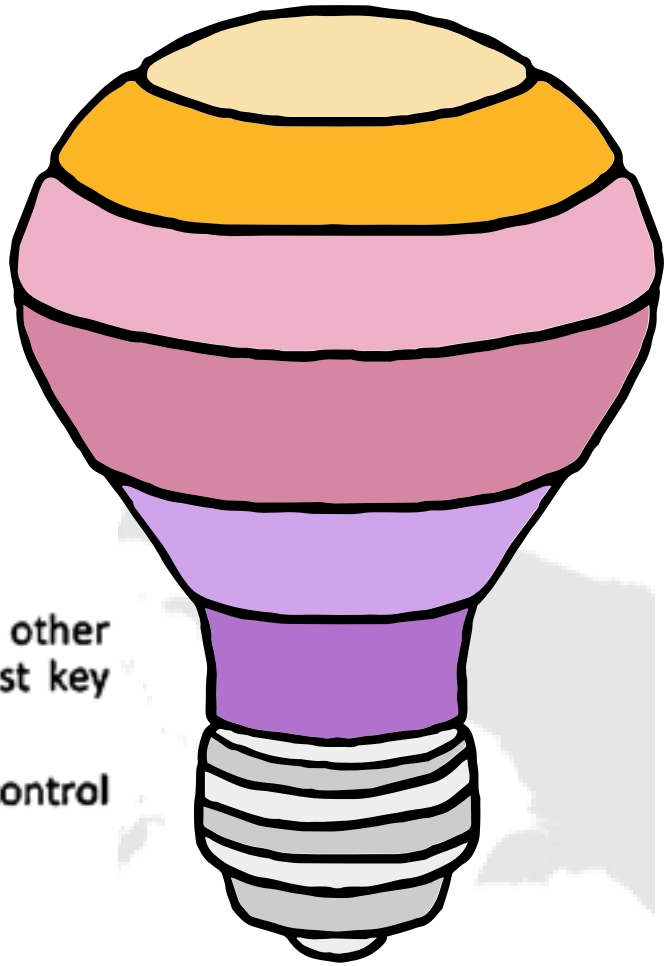
- To audit the auditee's ISMS documentation
- To evaluate physical locations and site-specific conditions and to determine the preparedness for the stage 2 audit
- To review the auditee status and understanding according to standard's requirements
- To collect necessary information, including statutory, legal and regulatory requirements
- To evaluate internal audits
- To prepare for Stage 2

It is recommended to conduct part of Stage 1 audit at auditee premises

STAGE 1 AUDIT - OUTPUT

- Audit schedule “the Stage 2” plan
- Verified ‘Scope’ statement
- Verified resources
- Verified ISMS documentation (Manual, Procedures)
- State of Management ‘Readiness’
- Findings of Evaluation

STAGE 2 AUDIT



Purpose of the stage 2

To evaluate the implementation, including effectiveness, of the client's management system.

The stage 2 audit shall take place at the site(s) of the client.

It shall include:

- information and evidence about conformity to all requirements of ISO 27001 standard or other normative document; performance monitoring, measuring, reporting and reviewing against key performance objectives and targets;
- the client's management system and performance as regards legal compliance; operational control of the client's processes;
- internal auditing and management review;
- management responsibility, etc.

BADAN SIBER DAN SANDI NEGARA

Memulai audit

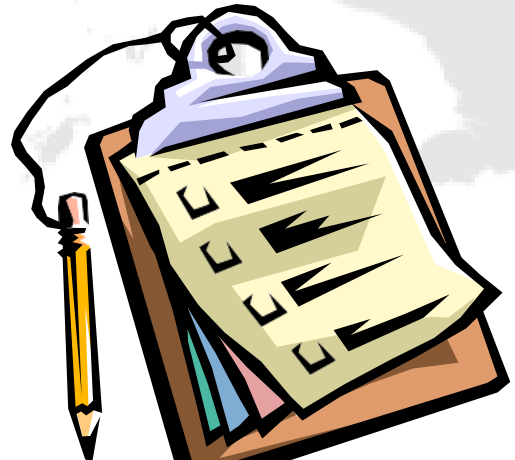
- menunjuk audit team leader
- definisi tujuan-tujuan audit, ruang lingkupdan kriteria
- menentukan kelayakan audit (*informasi audit plan, kerja sama dari auditee, waktu dan sumber daya*)
- menetapkan tim audit
- melakukan kontak awal dengan auditee

Catatan Audit

- Catatan Program Audit
  - lingkup dan tujuan program audit yang terdokumentasi
  - Risiko program audit
  - hasil tinjauan efektivitas program
- Catatan Hasil Audit
  - audit plan
  - laporan audit
  - laporan ketidaksesuaian
  - laporan tindakan koreksi
  - audit notes
  - hasil verifikasi
- Catatan Personnel
  - Evaluasi kompetensi dan kinerja auditor
  - Seleksi Tim Audit
  - Menjaga dan meningkatkan kompetensi

Notes:

Catatan sebaiknya dipelihara untuk menunjukan implementasi program audit sudah terpenuhi.



BADAN SIBER DAN SANDI NEGARA

Contoh Audit Plan

Company / Auditee	PT. XYZ
Audit Objective	Check QMS systems implementation
Audit Location	JL. Soekarno Hatta, Bandung
Auditee Representatives	MR and Division Head
Audit Scope	All Division
Audit Criteria	ISO 9001:2015
Date of Audit	26 – 30 Oktober 2015
Audit Leader	Sukamta (SKT) – Lead Auditor
Auditor	Ronaldo (RO) ,Torres (TR), Del Piero (DP)

DAY / TIME	AREA / ORGANIZATIONAL UNIT	AUDITEE	AUDITOR	RELATED CLAUSES TO ISO 9001:2015
Day One				
08:30 – 09.00	Opening Meeting	All	All Auditor	
09.00 – 10.00	Top Management	Director, Vice Director	All Auditor	4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 6.1, 6.2, 6.3, 7.1, 7.2, 7.3, 7.4, 9.3, 10.1
10.00 – 12.00	Quality and Document Control	MR	MS, RO	5.3, 6.2, 7.5, 9.1, 9.2, 10.2, 10.3
10.00 – 12.00	Human Resource Dept.	Head of HRD	TR, DP	5.3, 6.2, 7.1.2, 7.2, 7.3, 7.4, 9.1, 10.2, 10.3

BADAN SIBER DAN SANDI NEGARA

Persiapan dokumen kerja

Dokumen kerja sebaiknya disiapkan dan digunakan oleh Tim Audit sebagai referensi dan alat pencatatan hasil audit, termasuk :

- checklist and audit sampling plan
- form pencatatan ketidaksesuaian (Corrective Action Request/Report)

Catatan – catatan yang dihasilkan pada saat Audit Internal dilakukan, harus disimpan (lihat elemen 8.2.2 ISO 9001:2015)

BADAN SIBER DAN SANDI NEGARA

Poin Chekclist

- What – **aktivitas apa yang akan dicek/diverifikasi**
- Why – **tujuan pelaksanaan aktivitas (kesesuaian dengan target, kebijakan, prosedural, dll.)**
- Where – **informasi yang dibutuhkan terkait dengan pelaksanaan aktivitas yang diobservasi**
- When – **tenggat waktu pelaporan kinerja dan penyelesaian aktivitas sesuai target**
- Who – **orang/bagian/site yang bertanggungjawab atas pelaksanaan aktivitas terkait dan penanggungjawab tindak lanjut jika target tidak tercapai**
- How – **bagaimana aturan main pelaksanaan, pemantauan dan pengukuran keberhasilan aktivitas tersebut**

Ceklist Audit

Fungsinya yaitu:

Sebagai alat bantu mengingat klausul kriteria audit dari proses yang menjadi tugas auditor Untuk membantu auditor mengelola waktu pelaksanaan audit, karena waktu audit terbatas. Membantu bagi auditor baru agar dapat melaksanakan audit tetap dalam batasan proses dan kriteria yang menjadi bagian tugas nya.

Catatan:

Daftar ceklist audit sebenarnya bukanlah daftar pertanyaan yang harus diajukan dalam audit.

Seharusnya daftar periksa berisi:

Daftar klausul dari kriteria audit, ini digunakan oleh tim audit untuk memeriksa apakah semua klausul telah diaudit Daftar kata kunci dari semua persyaratan klausul yang relevan dengan proses yang menjadi bagian tugas auditor

Contoh Prosedur Audit

<<nama kontrol>>	
Observasi	<<isikan jawaban anda>>>
Dokumen	<<isikan jawaban anda>>>
Interviu	<<isikan jawaban anda>>>
Verifikasi Teknis	<<isikan jawaban anda>>>
Analisis	<<isikan jawaban anda>>>

Protection of logged information (A.12.4.2): Logging facilities and log information shall be protected against tampering and unauthorized access.	
Observation	Observation of protection measures implemented against sabotage and unauthorized accesses
Document	Documentation of controls in place to protect information logged against sabotage and unauthorized accesses, information logging policy and related procedures, intrusion test reports
Interview	Interview with the information security manager and validate the logging policy objectives, interview with the network administrator to validate the operation of the controls in place to protect the logged information against sabotage and unauthorized accesses
Technical verification	Observation of logging equipment configurations to verify their compliance to the organization's policies and procedures
Analysis	Analysis of a sample of logged information

Policies for information security (A.5.1.1)	
Observasi	
Dokumen	Documentation review of the information security policy to validate the content
Interviu	Interview with the person in charge of information security to validate the approval and distribution process of the policy
Verifikasi Teknis	Verification of the policy distribution media (Website, hard copy version, information in the employee manual, etc.)
Analisis	

Audit Finding

Apakah definisi temuan audit? Mengapa kalau saat closing meeting audit muncul temuan yang banyak maka kita merasa khawatir? Apakah temuan berarti kesalahan?

Temuan audit (audit finding) adalah **hasil evaluasi** atas bukti yang didapatkan dalam audit yang dibandingkan dengan **kriteria audit**. Saat melakukan audit, auditor melakukan investigasi untuk mendapatkan bukti-bukti penerapan sistem manajemen di organisasi. Setelah bukti-bukti penerapan didapatkan, kemudian auditor akan mengevaluasi apakah bukti tersebut memenuhi atau tidak memenuhi persyaratan/kriteria audit

Audit Finding

Jika bukti penerapan pada suatu proses SMKI (SNI ISO/IEC: 27001:2013) memenuhi persyaratan maka auditor menyimpulkan proses tersebut SESUAI dengan kriteria audit SMKI. Di saat inilah sudah muncul TEMUAN audit, karena SESUAI merupakan hasil evaluasi bukti penerapan dimana bukti tersebut memenuhi syarat SMKI, sehingga dikatakan Temuannya merupakan suatu KESESUAIAN.

Conformity

- Sesuai dengan permintaan standar/persyaratan

contoh:

- Tersedia dokumen akte pendirian perusahaan dan perubahan serta telah disahkan oleh Kemenhukham
- Telah memiliki IUP yang sesuai dengan kondisi perusahaan terkait jenis komoditi, luas kebun dan atau kapasitas PKS

Audit Finding

Sebaliknya, jika Bukti penerapan SMKI pada suatu proses tidak memenuhi persyaratan SNI ISO/IEC: 27001:2013, maka auditor menyimpulkan proses tersebut TIDAK SESUAI dengan kaidah SMKI. Ini juga sudah merupakan TEMUAN karena TIDAK SESUAI juga merupakan hasil evaluasi atas bukti penerapan, dimana auditor yakin bahwa bukti tersebut tidak memenuhi syarat SMKI. Temuannya merupakan sebuah KETIDAKSESUAIAN.

Contoh:

- Belum tersedia dokumen perubahan lahan(land trajectory) di PT X
- Belum tersedia prosedur pembukaan lahan (land clearing procedure) di PT Y
- Pengiriman TBS lebih dari 24 Jam dari Kebun C ke PKS periode 1 s/d 30 Januari 2019 sehingga tidak sesuai SOP & standard

Non-Conformity

Audit Finding

Lebih lanjut, dalam audit mungkin juga bertemu kondisi dimana bukti-bukti penerapan SMKI pada suatu proses sudah SESUAI dengan persyaratan SNI ISO/IEC: 27001:2013, tetapi menurut Auditor bisa ada praktik atau cara lain yang lebih baik/lebih efektif/lebih efisien dalam menerapkan SMKI pada proses tersebut. Pada situasi inilah muncul Temuan yang berupa PELUANG PENINGKATAN atau OPPORTUNITY FOR IMPROVEMENT (OFI).

- tidak dikategorikan ketidaksesuaian
- tidak melanggar elemen dari sistem manajemen mutu yang telah ditetapkan
- berdasarkan pengalaman dan pengetahuan seorang Auditor Internal
- bersifat saran untuk peningkatan atau peluang perbaikan

OFI

Contoh:

“Pelaksanaan diklat On-Job-Training sebaiknya mempertimbangkan waktu yang tepat untuk pelaksanaan dan evaluasinya.”

BADAN SIBER DAN SANDI NEGARA

Follow Up Audit

Pada tahap ini, auditi wajib melaksanakan tindakan perbaikan untuk semua ketidaksesuaian dari hasil audit.

Setelah dilakukan tindakan perbaikan maka dilakukan monitoring atas efektivitas tindakan perbaikan tersebut.

Jika sudah efektif maka ketidaksesuaian dapat di close out.

BADAN SIBER DAN SANDI NEGARA

End- Up Audit

Closing Meeting

Penyajian semua finding, secara. Fair,, Finding yg belum sesuai harus detail sebailiknyayg sudah cukup sekilas

Audit Finding

Semua catatan finding yg tidak sesuai harus terdokumentasi & dsampaikan. Finding hal yg harus diperbaiki, bukan dicari2 kesalahan

Audit Scope

extent and boundaries of an audit

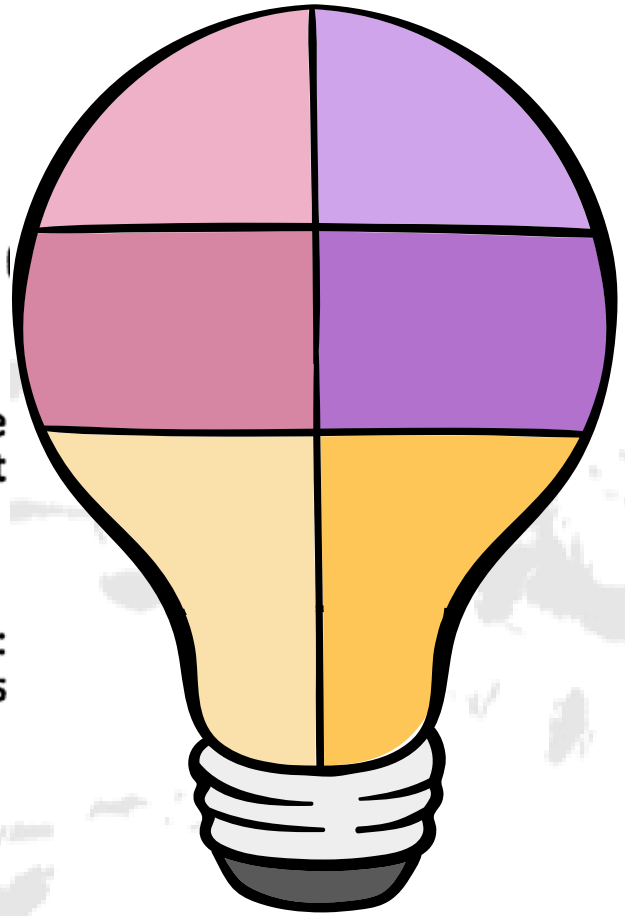
Audit Findings

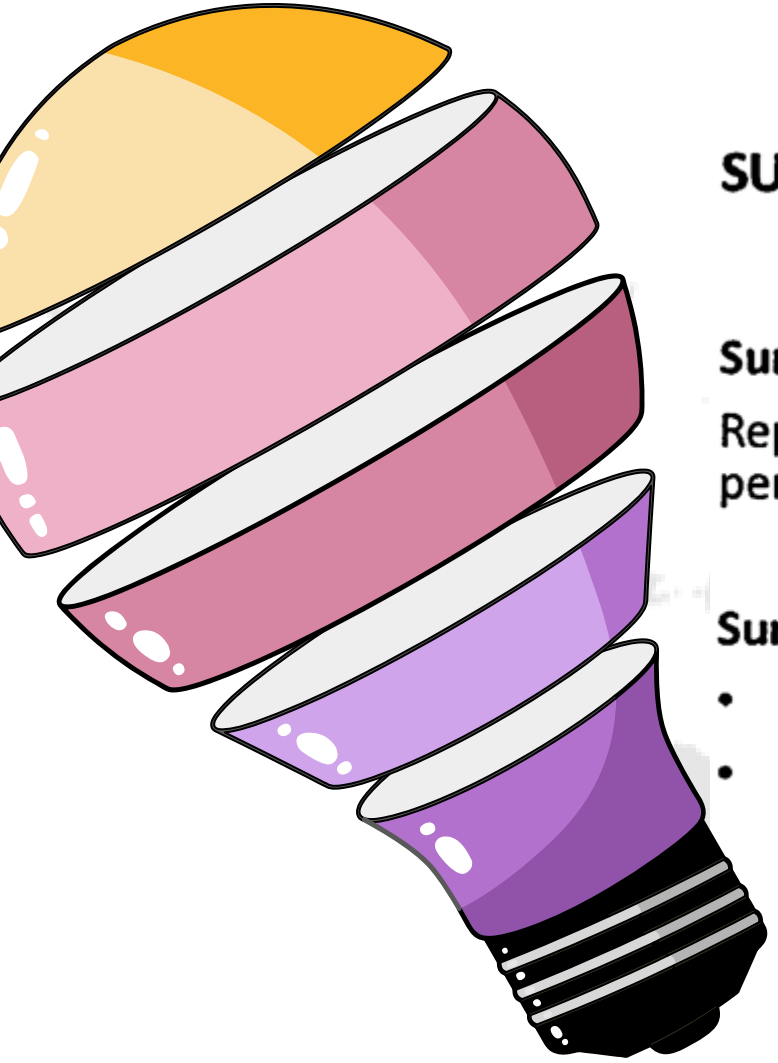
results of the evaluation of the collected audit evidence (3.3) against audit criteria

INITIAL CERTIFICATION AUDIT CONCLUSIONS

The audit team shall analyze all information and audit evidence gathered during the stage 1 and stage 2 audits to review the audit findings and agree on the audit conclusions.

The audit team shall provide to CB the information necessary for certification decision: the audit reports; comments on non-conformities; correction and corrective actions taken by clients; recommendations whether or not to grant certification.





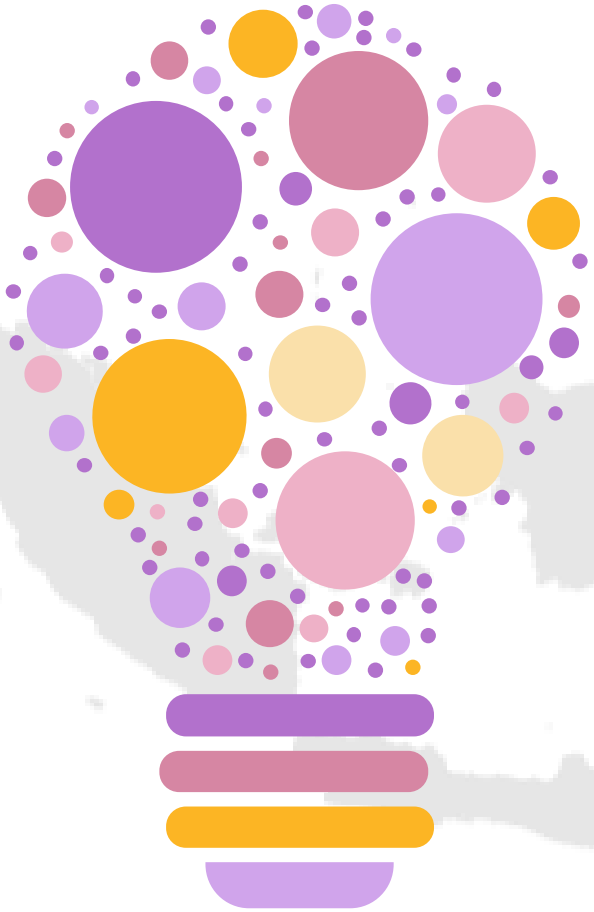
SURVEILLANCE

Surveillance activities

Representative areas and functions in the scope of ISMS shall be monitored at planned periods, taking into account changes at the client or the ISMS.

Surveillance audits

- On-site audit, not necessarily the full ISMS audits
- Shall be planned together with other surveillance activities in order to keep CB confident that the certified ISMS fulfils ISO 27001:2013 requirements



RECERTIFICATION

The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the ISMS as a whole, and its continued relevance and applicability for the scope of certification

It is a full ISMS audit; The recertification audit shall include an on-site audit information for granting recertification

The certification body shall make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification