TEKNIK AUDIT SISTEM INFORMASI / TEKNOLOGI INFORMASI

TEKNIK AUDIT

1. Audit Pengendalian *Entity-level*
2. Audit *data centers dan disaster recovery*
3. Audit switch, routers dan firewalls
4. Audit sistem operasi
5. Audit web server dan web aplikasi
6. Audit *database*
7. Audit penyimpanan (*Storage)*
8. Audit lingkungan virtual
9. Audit Wlan dan Mobile devices
10. Audit aplikasi
11. Audit *cloud computing dan Outsourced operations*
12. Audit proyek perusahaan/organisasi

AUDIT PENGENDALIAN ENTITY-LEVEL

Audit pada area TI, seperti :

1. Perencanaan strategis dan *technology roadmaps*
2. Indikator dan matriks kinerja
3. Persetujuan proyek dan proses pengawasan
4. Kebijakan, Standar dan Prosedur
5. Manajemen Karyawan
6. Manajemen Aset dan kapasitas
7. Konfigurasi sistem dan manajemen perubahan

PENDAHULUAN

- Pengendalian pada level entitas meresap di seluruh organisasi. Topik ini akan melingkupi seluruh organisasi.
- Bagian ini akan membantu Auditor untuk melihat secara keseluruhan dari perusahaan.
- Apa yang termasuk dan tidak termasuk dalam pengendalian level entitas tidak dapat selalu didefinisikan, tergantung bagaimana lingkungan TI nya.

MASTER CHECKLIST

Checklist untuk Audit Pengendalian Entity-level
1. Review keseluruhan struktur TI organisasi untuk memastikan bahwa hal tersebut memberikan pemberian tugas atas kewenangan dan tanggung jawab dari operasi TI dan pemisahan pekerjaan
2. Review proses perencanaan strategis TI untuk memastikan bhawa ia selaras dengan strategi bisnis. Evaluasi proses TI organisasi untuk mengawasi progress perencanaan strategis
3. Menetapkan apakah strategi teknologi dan aplikasi serta roadmap ada, dan evaluasi proses perencanaan teknis jangka panjang
4. Review indikator dan pengukuran kinerja TI. Pastikan bahwa proses dan matriks ada dan disetujui oleh stakeholder untuk mengukur kinerja aktivitas keseharian juga untuk melacak kinerja berdasarkan SLA, budget, dan kebutuhan operasional lainnya.
5. Review proses TI organisasi untuk menyetejui dan memprioritaskan proyek baru. Tetapkan apakah proses ini memadai untuk memastikan akuisisi sistem dan pengembangan proyek tidak dapat berjalan tanpa persetujuan. Pastikan manajemen dan stakeholder utama meninjau status proyek, jadwal, dan budget secara periodik melalui siklus proyek.
6. Evaluasi standar untuk mengelola eksekusi proyek TI dan untuk menjamin bahwa kualitas produk yang dikembangkan/didapatkan oleh organisasi. Tetapkan bagaimana standar tersebut disampaikan dan dijalankan.

MASTER CHECKLIST

Checklist untuk Audit Pengendalian Entity-level
7. Pastikan terdapat kenijakan keamanan TI dan menyediakan kebutuhan yang memadai untuk keamanan lingkungan. Tetapkan bagaimana kebijakan tersebut disampaikan dan bagaimana pemenuhan diawasi dan dijalankan.
8. Review dan evaluasi proses penilaian risiko untuk TI organisasi
9. Review dan evaluasi proses yang menjamin bahwa pegawai TI memiliki kemampuan dan pengetahuan yang dibutuhkan untuk melaksanakan pekerjaan mereka
10. Review dan evaluasi kebijakan dan proses untuk menentukan kepemilikan data perusahaan, klasifikasi data, perlindungan data sesuai klasifikasi, serta siklus hidup data
11. Pastikan terdapat proses efektif untuk mematuhi hukum dan peraturan yang berdampak pada TI dan untuk mempertahankan kepedulian ats perubahan pada lingkungan regulasi.
12. Review dan evaluasi proses untuk menjamin bahwa end-user di lingkungan TI memiliki kemampuan untuk melaporkan masalah, dan terlibat dalam pengambilan keputusan TI, serta merasa puas dengan pelayanan yang diberikan TI
13. Review dan evaluasi proses untuk mengelola layanan pihak ketiga, menjamin bahwa peran dan tanggung jawab mereka didefinisi dengan jelas dan pengawasan kinerja mereka

MASTER CHECKLIST

Checklist untuk Audit Pengendalian Entity-level
14. Review dan evaluasi proses untuk mengendalikan non-employee logical access
15. Review dan evaluasi proses untuk menjamin bahwa perusahaan memenuhi lisensi software
16. Review dan evaluasi pengendalian atas remote access di jaringan organisasi
17. Pastikan bahwa rekrutmen dan pemberhentian prosedur jelas dan komprehensif
18. Review dan evaluasi kebijakan dan prosedur untuk mengendalikan pengadaan dan perpindahan hardware
19. Pastikan bahwa konfigurasi sistem dikendalikan dengan manajemen perubahan untuk menghindari berhentinya suatu pekerjaan
20. Pastikan bahwa media transportasi, penyimpanan, penggunaan kembali, dan penghancuran ditangani degan kebijakan dan prosedur organisasi
21. Verifikasi kapasitas pengawasan dan perencanaan dengan kebijakan dan prosedur
22. Berdasarkan struktur dan proses struktur organisasi, identifikasi dan audit proses pada level entitas TI lainnya

1. REVIEW KESELURUHAN STRUKTUR TI ORGANISASI

LANGKAH PENGUJIAN

- Struktur organisasi TI yang tidak didefinisikan dengn baik akan berakibat tidak jelasnya tanggung jawab, yang menyebabkan fungsi-fungsi tidak dapat bekerja dengan efektif dan efisien.
- Jika batas kewenangan/otoritas tidak dibuat, akan menrujuk pada ketidakepakatan atas siapa yang memiliki kemampuan untuk membuat keputusan akhir.
- Jika tugas-tugas TI tidak dipisahkan dengan baik, akan memicu aktivitas kecurangan dan mempengaruhi integritas dari proses dan informasi organisasi

1. REVIEW KESELURUHAN STRUKTUR TI ORGANISASI

CARA MENGUJI

1. Tinjau chart TI organisasi dan pastikan bahwa telah ada struktur pelaporan yang jelas.
2. Tinjau chart dan charter TI organisasi dan pastikan bahwa sudah dapat menggambarkan area tanggung jawab. Tentukan apakah sudah jelas bagaimana tenggung jawab dibagi di dalam organisasi, atau evaluasi apakah ada peluang terjadi kebingungan dan overlap. Pertimbangkan juga wawancara dengan pegawai TI atau konsumen.
3. Evaluasi divisi tanggung jawab di dalam organisasi TI untuk menjamin bahwa tugas dipisahkan dengan baik.

1. REVIEW KESELURUHAN STRUKTUR TI ORGANISASI

PANDUAN DASAR DALAM MENINJAU

1. Pegawai TI tidak seharusnya melakukan input data/data entry
2. Programmer dan pihak lain yang bertugas mengerjakan run/maintain dukungan terhadap sistem tidak seharusnya bisa secara langsung melakukan modifikasi kode, data, atau struktur penjadwalan pekerjaan
3. Programmer dan pihak lain yang mengerjakan run/maintain dukungan terhadap sistem tidak seharusnya dipisahkan dari pihak-pihak yang menjalankan dukungan terhadap operasi TI
4. Keamanan TI organisasi harus bertanggung jawab untuk membuat kebijakan, serta melakukan pengawasan untuk pemenuhan kebijakan

2. REVIEW PROSES PERENCANAAN STRATEGIS TI

- Untuk mendapatkan efektivitas jangka panjang, TI organisasi harus memiliki strategi menyangkut rencana ke depan, bagaimana agar organisasi dapat memberikan reson yang cepat terhadap perubahan, di mana masalah sering timbul dan bagaimana mengatasinya.
- Organisasi harus menyadari akan adanya kebutuhan bisnis mendatang dan perubahan dalam lingkungan.
- Prioritas TI juga penting untuk selaras dengan prioritas bisnis.

2. REVIEW PROSES PERENCANAAN STRATEGIS TI

CARA MENGUJI

1. Carilah bukti adanya perencanaan strategis pada TI dan pahami bagaimana perencanaan dijalankan.
2. Tentukan bagaimana strategi dan prioritas organisasi digunakan dalam mengembangkan strategi dan prioritas TI.
3. Review dokumentasi prioritas TI jangka pendek dan jangka panjang
4. Evaluasi proses yang ada untuk mengawasi progress dari prioritas secara periodik, serta evaluasi kembali dan update prioritas tersebut.

3. MENENTUKAN KEBERADAAN ROADMAP DAN STRATEGI TI DAN APLIKASI

CARA MENGUJI

TI merupakan lingkungan yang cepat berubah dan penting bagi organisasi untuk memahami dan merencanakan menghadapi perubahan

1. Carilah bukti bahwa perencanaan teknik jangka panjang dijalankan.
2. Untuk pembelian aplikasi dan teknologi tentukan apakah organisasi memahami dukungan dari vendor
3. Tentukan apakah ada proses untuk mengawasi perubahan yang signifikan, pertimbangkan bagaimana perubahan tersebut akan berdampak pada perusahaan, serta carilah peluang untuk menggunakan teknologi baru yang dapat membantu organisasi

4. REVIEW INDIKATOR DAN PENGUKURAN KINERJA TI

CARA MENGUJI

TI organisasi ada untuk mendukung bisnis dan operasional sehari-hari. Jika standar minimal atas kinerja tidak ditetapkan dan diukur, akan sulit bagi bisnis untuk mengetahui apakah layanan TI organisasi dikerjakan dengan baik.

1. Dapatkan kopi dari pengukuran apapun yang ada pada aktivitas rutin TI organisasi. Kemudian tentukan tujuan dari pengukuran tersebut dan pastikan apakah stakeholder menyetujui adanya matriks tersebut.
2. Review SLA yang ada untuk mendukung TI stakeholder utama. Pastikan bahwa ada proses untuk mengukur kinerja nyata terhadap SLA
3. Pastikan ada proses untuk menyusun bugdet dan pemenuhan TI organisasi terhadap budget. Dapatkan kopian budget TI saat ini dan beberapa tahun ke depan, juga dokumen analisa budget vs kenyataan.

5. REVIEW PROSES PRIORITAS PROYEK TI

CARA MENGUJI

Tanpa proses persetujuan dan prioritas proyek baru TI yang terstruktur, sumberdaya TI kemungkinan tidak akan digunakan secara efisien. Juga bisa jadi proyek TI tidak akan bisa memenuhi kebutuhan bisnis.

1. Review dokumentasi yang ada mengenai proposal proyek dan proses persetujuan.
2. Evaluasi proses untuk kemungkinan adanya proyek tanpa persetujuan
3. Cari bukti bahwa proyek yang diusulkan elah melalui proses prioritas
4. Review bukti manajemen dan stakeholder utama secara periodik meninjau status, budget dan jadwal dari proyek TI yang aktif.
5. Pastikan bahwa proses persetujuan proyek melalui proses analisa biaya sebelum proyek dijalankan.

6. EVALUASI STRANDAR TATA KELOLA ESEKUSI PROYEK TI

CARA MENGUJI

Jika standar tidak ada dan tidak dijalankan dalam lingkungan TI, proyek akan dieksekusi dengan tidak disiplin, masalah kualitas akan muncul dalam pengembangan dan pembelian produk, dan lingkungan TI akan melebar (peningkatan biaya pendukung, dll)

Tetapkan apakah ada dokumen standar seperti,

1. Manajemen proyek
2. Pengembangan software : standar dalam coding, misal, pemberian nama, history, komentar,dll.
3. Konfigurasi sistem : standar konfigurasi laptop, desktop, server, dll
4. Hardware dan software : standar penggunaan hardware dan software
5. Standar jaminan kualitas

7. MEMASTIKAN KEBERADAAN KEBIJAKAN KEAMANAN TI

- Jika kebijakan tidak ada atau tidak dapat memberikan cakupan yang cukup, pegawai terpaksa akan menetapkan aturan yang dibuat sendiri terkait isu keamanan.
- Jika ada kebijakan tetapi tidak disampaikan kepada pegawai, mereka tidak akan mengikuti kebijakan tersebut.
- Jika kebijakan dijalankan tetapi tidak diawasi, pegawai akan “belajar” bahwa tidak ada konsekuensi jika tidak mengikuti kebijakan tersebut.

7. MEMASTIKAN KEBERADAAN KEBIJAKAN KEAMANAN TI

CARA MENGUJI

1. Verifikasi cakupan kebijakan
   - Dapatkan kopi kebijakan TI organisasi
   - Review kebijakan berdasarkan standar industri
2. Verifikasi keterlibatan stakeholder
   - Pastikan stakeholder utama dilibatkan dalam penyusunan kebijakan.
   - Dapatkan daftar pegawai yang dilibatkan dalam pembuatan dan persetujuan kebijakan keamanan TI
3. Verifikasi proses di sekitar kebijakan
   - Review proses peninjauan dan pembaharuan kebijakan untuk menjamin bahwa organisasi bisa mengikuti perubahan
   - Review proses evaluasi perubahan lingkungan yang akan mempengaruhi perkembangan kebijakan baru
   - Pastikan ada ketentuan yang dibuat untuk mendapatkan pengecualian dari kebijakan
   - Review proses implementasi keamanan TI untuk memenuhi kebijakan
   - Pastikan ada mekanisme untuk pegawai melaporakan insiden keamanan atau kekhawatiran yang diikuti dengan resolusi.

8. REVIEW PROSES PENILAIAN RISIKO

CARA MENGUJI

Tanpa proses penilaian risiko, TI organisasi tidak akan tahu akan risiko yang mungkin terjadi dalam proses pencapaian tujuan, kemudian tidak akan bisa mempersiapkan diri untuk menghadapi risiko.

- Carilah bukti bahwa organisasi secara periodik mempertimbangkan risiko yang mungkin terjai dalam lingkungan TI dan membuat keputusan antara menerima, mitigasi atau menghindari risiko tersebut.

9. REVIEW DAN EVALUASI KEMAMPUAN STAFF TI

CARA MENGUJI

Jika staff TI tida berkualifikasi untuk melaksanakan pekerjaannya, maka akan berdampak buruk pada layanan TI yang dihasilkan. Jika mekanisme tidak ada untuk mempertahankan dan meningkatkan pengetahuan serta kemampuan staff, maka pengetahuan dan kemampuan mereka akan tertinggal.

- Review kebijakan dan proses HR menyangkut staff TI. Carilah mekanisme yang memastikan bahwa organisasi hanya mempekerjakan orang dengan kualifikasi dan kemampuan, serta menyediakan kesempatan untuk meningkatkan kemampuan dan pengetahuan staff

10. REVIEW DAN EVALUASI KEBIJAKAN DAN PROSES DATA

CARA MENGUJI

Kebijakan dan proses yang menyangkut : kepemilikan data, klasifikasi data, perlindungan data sesuai dengan klasifikasinya.

1. Review kebijakan klasifikasi data organisasi. Kebijakan tersebut harus memuat identifikasi kepemilikan data penting, framework untuk klasifikasi data berdasarkan tingkat sensitivitasnya (rahasia, data internal, data publik). Kebijakan juga harus memuat spesifikasi masing-masing level klasifikasi dan cara melindunginya.
2. Review bukti bahwa kebijakan klasifikasi data telah dilaksanakan.

11. PASTIKAN KEBERADAAN PROSES PEMENUHAN HUKUM

CARA MENGUJI

1. Carilah pihak yang bertanggung jawab untuk mengawasi lingkungan regulasi yang mungkin akan berdampak pada TI
2. Review proses yang digunakan untuk mengawasi lingkungan regulasi, dan evaluasi keefektivitasannya.
3. Dapatkan daftar peraturan TI yang telah diiedntifikasi dan carilah bukti bahwa organisasi telah memenuhi peraturan tersebut

12. REVIEW DAN EVALUASI PROSES PADA END-USER

CARA MENGUJI

Lingkungan TI ada untuk mendukung staff dalam melaksanakan pekerjaan, maka penting adanya proses dimana staff dapat memberikan masukan untuk kualitas layanan yang mereka terima.

1. Pastikan bahwa help-desk berfungsi sebagai wadah bagi end-user melaporkan jika terjadi masalah
2. Pastikan terdapat proses untuk mendapatkan feedback dari end-user setelah masalah selesai.
3. Review SLA yang ada untuk mendukung TI stakeholder. Pastikan juga terdapat proses untuk mengukur pencapaian SLA

13. REVIEW&EVALUASI PROSES PENGELOLAAN PIHAK KETIGA

CARA MENGUJI

Banyak organisasi melakukan outsource TI mereka, contoh, web server hosting, system support, pragramming, dll. Jika vendor ini tidak dikelola, akan menuju pada buruknya layanan di lingkungan TI

1. Review proses pemilihan vendor
2. Pastikan kontrak dengan pihak ketiga secara spesifik menjelaskan peran dan tanggung jawab dari vendor, dan SLA. Review contoh kontrak dengan pihak ketiga untuk mengetahuinya,
3. Pastikan kontrak berisi klausa nondisclosure, yang mencegah vendor membocorkan informasi tentang organisasi.
4. Review proses untuk mengawasi jalannya pemberian layanan oleh pihak ketiga

14. REVIEW&EVALUASI PROSES AKSES LOGIS NON-PEGAWAI

CARA MENGUJI

Kebanyakan organisasi mempekerjakan pekerja kontrak dan outsourcing juga melakukan kerja sama dengan pihak ketiga. Jika akses informasi mereka tidak dikelola, serta batasan penggunaan informasi tidak disampaikan, dikhawatirkan aset informasi organisasi akan terexposed keluar dan disalahgunakan.

1. Pastikan terdapat kebijakan [ersetujuan dari staff kepada non-staff saat akan mengakses informasi
2. Review dan evaluasi proses penyampaian kebijakan kepada non-staff, sebelum memberikan mereka ijin akses
3. Review dan evaluasi proses penghapusan akses logis non-staff ketika ia terbukti menyalahgunakan informasi
4. Pastikan non-staff menandatangani NDA, agar ada jaminan legal atas perlindungan aset informasi
5. Pastikan agar mempertimbangkan pemberian klasifikasi data mana saja yang boleh dan tidak boleh di akses oleh non-staff

15. REVIEW&EVALUASI PROSES PEMENUHAN LISENSI

CARA MENGUJI

Menggunakan software secara ilegal akan berujung pada penalti, dan lawsuit. Saat ini dengan mudah staff dapat mengunduh software dari internet, organisasi perlu mengembangkan proses untuk mencegah aktivitas ini.

- Carilah bukti bahwa organisasi mempertahankan daftar lisensi software (Microsoft Office, aplikasi ERP, dll), dan mengembangkan proses pengawasan penggunaan lisensi.

16. REVIEW&EVALUASI PENGENDALIAN REMOTE ACCESS

CARA MENGUJI

1. Pastikan User ID dan Password dibutuhkan untuk Remote Access dan data ditukarkan melalui jaringan yang aman
2. Tentukan apakah ada proses persetujuan untuk menjalankan remote access terutama bagi non-staff
3. Evaluasi pengendalian yang menjamin bahwa koneksi eksternal dengan partner bisnis dihapus/ditiadakan saat tidak lagi dibutuhkan
4. Evaluasi pengendalian yang menjamin unauthorized connections tidak dapat dilakukan ke dalam jaringan dan deteksi jika terdapat upaya tersebut
5. Pastikan kenijakan memberikan keamanan minimum yang harus dimiliki oleh semua perangkat untuk mengakses jaringan remotely

17. PASTIKAN PROSEDUR HIRING DAN TERMINATION JELAS

CARA MENGUJI

1. Review kebijakan dan prosedur HR untuk merekrut dan memberhentikan pegawai
2. Pastikan prosedur rekrutmen termasuk, background check, tes NAPZA dll
3. Pastikan prosedur pemberhentian termasuk penghentian akses logis dan fisik, pengembalian peralatan milik organisasi

18. REVIEW&EVALUASI KEBIJAKAN DAN PROSEDUR PENGADAAN

CARA MENGUJI

- Review dan evaluasi kebijakan dan prosedur pengadan dan pemindahan hardware
- Review dan evaluasi kebijakan dan prosedur manajemen aset organisasi dan pastikan kebijakan tersebut melingkupi :
  - Proses pengadaan aset, prosedur sebelum membeli hardware
  - Pelacakan aset, manajemen aset dan database penggunaan aset
  - Inventarisasi peralatan
  - Prosedur pemindahan dan penghancuran/menghilangkan aset

19. PASTIKAN KONFOGURASI DAN PENGENDALIAN SISTEM

CARA MENGUJI

Manajemen perubahan konfigurasi berguna untuk menjamin bahwa sistem dikendalikan dan dilacak untuk mengurangi risiko sistem. Termasuk di dalamnya, perencanaan, penjadwalan, penerapan, pelacakan perubahan terhadap sistem untuk mengurangi risiko akibat perubahan lingkungan.

- Pastikan bahwa prosedur manajemen konfigurasi berisi:
  - Permintaan perubahan
  - Menentukan secara spesifik apa yang harus diubah
  - Prioritas dan persetujuan usulan perubahan
  - Penjadwalan perubahan
  - Pengujian dan persetujuan sebelum penerapan, komunikasi rencana perubahan sebelum diterapkan
  - Penerapan perubahan
  - Penghapusan.menghilangkan perubahan jika ternyata tidak dapat bekerja dengan baik

20. PASTIKAN ADA KEBIJAKAN DAN PROSEDUR PENGGUNAAN MEDIA

CARA MENGUJI

Media trasportasi, penyimpanan, penggunaanan dan penghapusan.

Pengendalian media menjamin bahwa informasi yang disimpan dalam media penyimpanan tetap terjaga kerahasiaannya dan terlindungi dari pengrusakan dini.

- Pastikan terdapat kebijakan dan prosedur mengenai :
  - Kebutuhan enkripsi informasi yang sensitif sebelum diberikan kepada pihak ketiga
  - kebutuhan pelatihan user tentang bagaimana menyimpan dan menghapus media
  - Kebutuhan media penyimpanan disimpan di tempat yang aman, dikendalikan temperaturnya.

21. VERIFIKASI KAPASITAS PENGAWASAN DAN PERENCANAAN

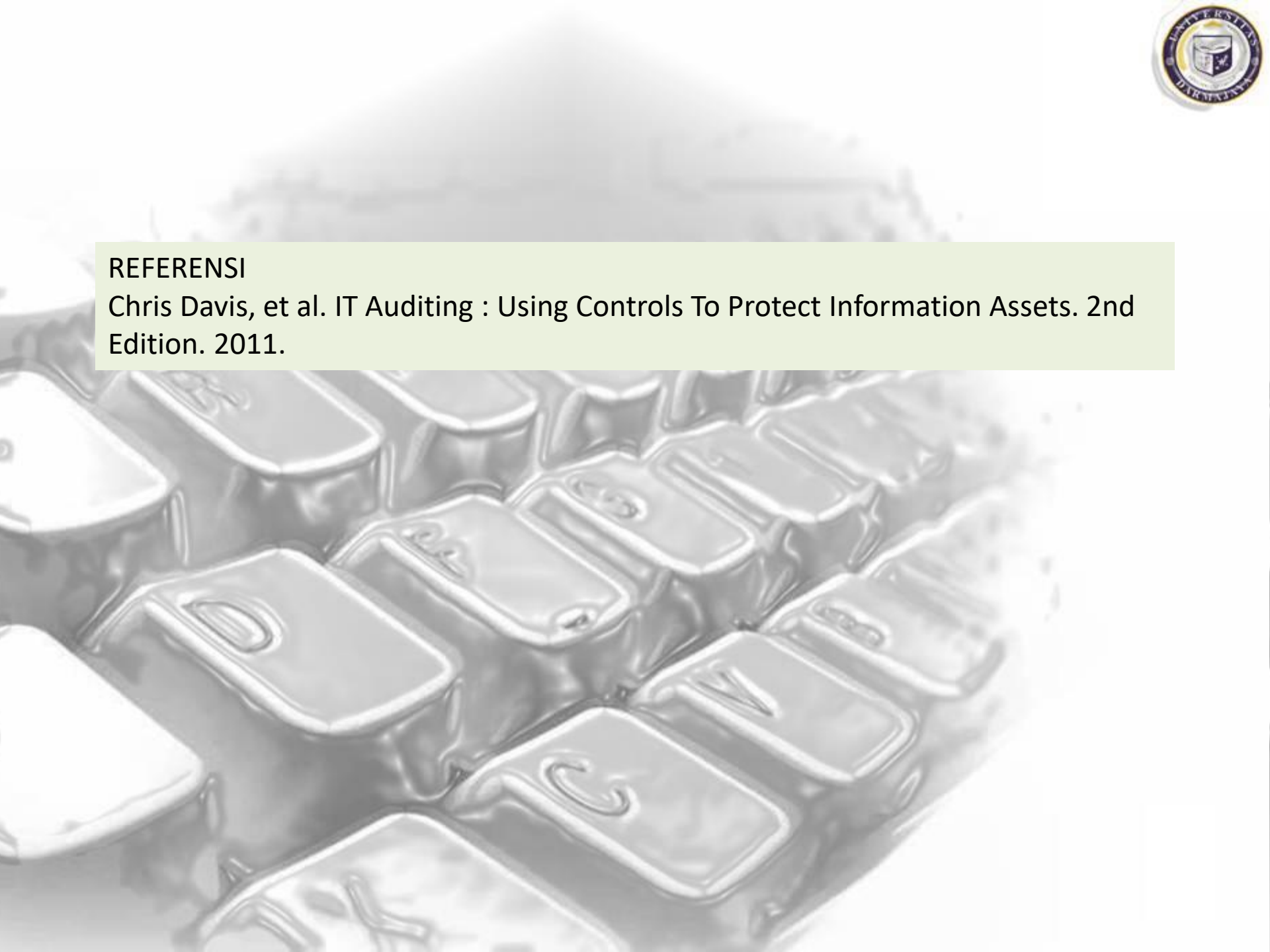
CARA MENGUJI

- Antisipasi dan pengawasan kapasitas dari fasilitas data center, sistem komputer dan aplikasi untuk menjamin ketersediaan sistem.
- Review :
  - Dokumen arsitektur untuk menjamin sistem dan fasilitas dirancang sesuai kebutuhan
  - Prosedur pengawasan sistem
  - Laporan ketersediaan sistem untuk menjamin masalah kapasitas sistem tidak menyebabkan downtime.

21. VERIFIKASI KAPASITAS PENGAWASAN DAN PERENCANAAN

CARA MENGUJI

- Antisipasi dan pengawasan kapasitas dari fasilitas data center, sistem komputer dan aplikasi untuk menjamin ketersediaan sistem.
- Review :
  - Dokumen arsitektur untuk menjamin sistem dan fasilitas dirancang sesuai kebutuhan
  - Prosedur pengawasan sistem
  - Laporan ketersediaan sistem untuk menjamin masalah kapasitas sistem tidak menyebabkan downtime.



REFERENSI

Chris Davis, et al. IT Auditing : Using Controls To Protect Information Assets. 2nd Edition. 2011.