ISBN 978-623-198-308-4

KONTROL DAN AUDIT TEKNOLOGI INFORMASI

Wahyuddin S, Nono Heryana, Alexander Waworuntu, Abdurrasyid, Angga Aditya Permana, Rima Rizqi Wijayanti, Santo Fernandi Wijaya, Suwito Pomalingo, Alfrian C Talakua, Agung Susilo Yuda Irawan, Luluk Tri Harinie, Wirawan Istiono

KONTROL DAN AUDIT TEKNOLOGI INFORMASI

Wahyuddin S
Nono Heryana
Alexander Waworuntu
Abdurrasyid
Angga Aditya Permana
Rima Rizqi Wijayanti
Santo Fernandi Wijaya
Suwito Pomalingo
Alfrian C Talakua
Agung Susilo Yuda Irawan
Luluk Tri Harinie
Wirawan Istiono

PT GLOBAL EKSEKUTIF TEKNOLOGI

KONTROL DAN AUDIT TEKNOLOGI INFORMASI

Penulis :
Wahyuddin S
Nono Heryana
Alexander Waworuntu
Abdurrasyid
Angga Aditya Permana
Rima Rizqi Wijayanti
Santo Fernandi Wijaya
Suwito Pomalingo
Alfrian C Talakua
Agung Susilo Yuda Irawan
Luluk Tri Harinie
Wirawan Istiono

ISBN : 978-623-198-308-4

Editor : Diana Purnama Sari, M.E
Penyunting : Tri Putri Wahyuni,S.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : PT GLOBAL EKSEKUTIF TEKNOLOGI
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jl. Pasir Sebelah No. 30 RT 002 RW 001
Kelurahan Pasie Nan Tigo Kecamatan Koto Tangah
Padang Sumatera Barat
Website : www.globaleksekutifteknologi.co.id
Email : globaleksekutifteknologi@gmail.com

Cetakan pertama, Mei 2023

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku Kontrol Dan Audit Teknologi Informasi Ini.

Buku Ini Membahas . Konsep dan Pengenalan IT Audit & Kontrol, Membangun IT Audit Internal yang Efektif, Metode dan Proses Audit IT, Audit Menggunakan CAAT (*Computer Assisted Audit Tools*), Teknik Audit Perangkat Keras, Teknik Audit Perangkat Lunak, Audit Pada Manajemen Proyek IT, Framework dan Standar Audi, Manajemen Risiko, Penetapan IT yang Efektif dan Lingkungan Keamanan, Keberlangsungan Perencanaan Bisnis, *Quality Assurance* dan ASQ Standard.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, Mei 2023

Penulis

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **ii**
DAFTAR GAMBAR ..... **x**
DAFTAR TABEL ..... **xi**
BAB 1 KONSEP DAN PENGENALAN IT AUDIT DAN KONTROL **1**
1.1 Pendahuluan 1
1.2 Konsep IT Audit 3
1.3 Tipe IT Audit 4
1.4 Kategori Utama IT Audit 5
1.5 Contoh Tipe IT Audit 6
1.6 Aplikasi IT Audit & Kontrol 8
1.7 Framework COBIT 5 9
DAFTAR PUSTAKA 11
BAB 2 MEMBANGUN IT AUDIT INTERNAL YANG EFEKTIF **13**
2.1 Pendahuluan 13
2.1.1 Definisi IT Audit Internal 13
2.1.2 Manfaat dari IT Audit Internal yang efektif 15
2.2 Persiapan IT Audit Internal 15
2.2.1 Membentuk Tim IT Audit Internal 15
2.2.2 Memahami Lingkup Audit 17
2.2.3 Menentukan Sumber Daya dan Anggaran 18
2.2.4 Memilih Metodologi Audit yang Sesuai 19
2.3 Pemahaman Lingkungan TI Perusahaan 20
2.3.1 Evaluasi Infrastruktur TI 20
2.3.2 Menganalisis Sistem Aplikasi yang Digunakan 21
2.3.3 Memahami Proses Bisnis 21
2.4 Identifikasi Risiko TI 22
2.4.1 Melakukan Identifikasi Risiko 22

2.4.2 Mengklasifikasikan Risiko 22
2.4.3 Menganalisis Dampak dan Kemungkinan Terjadinya Risiko 22
2.5 Penetapan Prioritas dan Rencana Audit 23
2.5.1 Menentukan Prioritas Risiko 23
2.5.2 Menentukan Rencana Audit 24
2.6 Pelaksanaan Audit 24
2.6.1 Melakukan Audit 24
2.6.2 Mengevaluasi Keamanan Sistem 25
2.6.3 Mengevaluasi Pengelolaan Data 25
2.6.4 Melakukan Pengujian Aplikasi 26
2.7 Pelaporan Hasil Audit 26
2.7.1 Membuat Laporan Hasil Audit 26
2.7.2 Menyampaikan Laporan Hasil Audit 26
2.7.3 Menentukan Tindak Lanjut dari Hasil Audit 27
2.8 Monitoring dan Evaluasi 27
2.8.1 Menentukan Program Monitoring dan Evaluasi 27
2.8.2 Menilai Efektivitas Audit Internal TI 27
2.8.3 Memperbaiki Proses Audit Internal TI 28
DAFTAR PUSTAKA 29
BAB 3 METODE DAN PROSES AUDIT TEKNOLOGI INFORMASI 33
3.1 Pendahuluan 33
3.2 Tujuan Audit TI 34
3.3 Metodologi Audit TI 37
3.3.1 Perencanaan (*Planning*) 37
3.3.2 Penilaian Resiko (*Risk Assessment*) 39
3.3.3 Evaluasi Kontrol (*Control Evaluation*) 41
3.3.4 Pengujian (*Testing*) 44
3.3.5 Pelaporan (*Reporting*) 46
3.3.6 Tindak Lanjut (*Follow-up*) 49
3.4 Kesimpulan 51

DAFTAR PUSTAKA 54
BAB 4 AUDIT MENGGUNAKAN CAAT 55
4.1 Pendahuluan 55
4.2 Fungsi Audit 57
4.2.1 Item-item untuk kepentingan audit..... 57
4.2.2 Audit perhitungan 58
4.2.3 Analisis Data 59
4.3 CAAT untuk Pengambilan Sampel 63
4.3.1 Sampling Atribut Acak dan Sampling Variabel..... 63
4.4 CAAT untuk Tinjauan Aplikasi 67
4.4.1 *Audit Command Language* (ACL) 68
4.5 CAAT untuk Audit Pengendalian Aplikasi 75
4.5.1 Pengendalian Spreadsheet 77
4.5.2 Pengendalian Database..... 78
4.6 CAAT untuk Mereview Operasional..... 79
4.7 Audit di Sekitar Komputer Versus Audit Melalui Komputer 80
DAFTAR PUSTAKA 89
BAB 5 TEKNIK AUDIT PERANGKAT KERAS 91
5.1 Pendahuluan 91
5.2 Hal – hal Penting Dalam Audit Perangkat Keras 92
5.3 Perangkat Keras Komputer 99
5.4 Perangkat Keras Infrastruktur 100
5.5 Tujuan Audit Perangkat Keras 102
5.6 Persiapan Audit Perangkat Keras 103
5.7 Orang yang Terlibat didalam Audit Perangkat Keras 105
5.8 Penyebab Kegagalan Audit Perangkat Keras..... 109
DAFTAR PUSTAKA 112
BAB 6 TEKNIK AUDIT PERANGKAT LUNAK 113
6.1 Pendahuluan 113
6.2 Apa itu audit perangkat lunak?..... 113

6.3 Mengapa audit perangkat lunak diperlukan? 115
6.4 Jenis audit perangkat lunak 117
6.5 Cara melakukan audit perangkat lunak 119
6.6 Pedoman Pelaksanaan Audit Perangkat Lunak 121
6.7 Daftar periksa audit perangkat lunak 124
6.8 Setelah audit perangkat lunak 127
DAFTAR PUSTAKA 128
BAB 7 AUDIT PADA MANAJEMEN PROYEK IT 129
7.1 Pendahuluan 129
7.2 Apa itu Audit? 130
7.3 Audit TI 131
7.4 Tahapan Audit TI 134
7.5 Mengapa Audit Manajemen Proyek TI penting? 135
7.6 Manajer Proyek 136
7.7 Manajemen Proyek Agile 137
DAFTAR PUSTAKA 139
BAB 8 FRAMEWORK DAN STANDAR AUDIT 141
8.1 Pendahuluan 141
8.2 COBIT (*Control Objectives for Information and Related Technologies*) 142
8.2.1 COBIT 142
8.2.2 Prinsip COBIT 143
8.2.3 Komponen Utama COBIT 144
8.2.4 Penerapan COBIT dalam Organisasi 145
8.3 ITIL (*Information Technology Infrastructure Library*) 145
8.3.1 Pengantar ITIL 145
8.3.2 Prinsip-prinsip ITIL 146
8.3.3 Siklus Manajemen Layanan ITIL 147
8.3.4 Service Value Chain ITIL 4 149
8.3.5 ITIL 4 *Practice* 150
8.3.6 Implementasi ITIL 151

8.4 ISO/IEC 27001:2013 (Sistem Manajemen Keamanan Informasi) 153
8.4.1 ISO/IEC 27001 :2013 153
8.4.1 Aspek Penting dalam ISO/IEC 27001 :2013 154
8.5 ISACA (*Information Systems Audit and Control Association*) 156
8.6 NIST (*National Institute of Standards and Technology*) 157
DAFTAR PUSTAKA 158
BAB 9 MANAJEMEN RISIKO 159
9.1 Pengenalan 159
9.2 Karakteristik Risiko 161
9.2.1 Ketidakpastian 161
9.2.2 Kerugian 163
9.3 Klasifikasi Risiko 164
9.3.1 Risiko Murni 164
9.3.2 Risiko Spekulatif 164
9.3.3 Risiko Keuangan 164
9.3.4 Risiko Operasional 165
9.3.5 Risiko Teknologi Informasi 165
9.4 Proses manajemen risiko 169
DAFTAR PUSTAKA 178
BAB 10 PENETAPAN IT YANG EFEKTIF DAN LINGKUNGAN KEAMANAN 181
10.Pendahuluan 181
10.2 Memahami Risiko Keamanan IT 181
10.2.1 Mengidentifikasi ancaman & risiko keamanan IT 182
10.2.2 Memahami dampak keamanan IT yang tidak terkendali 184
10.2.3 Mengukur Tingkat Risiko IT dalam Organisasi 185
10.3 Penetapan IT yang Efektif 186

10.3.1 Menentukan Kebutuhan dan Tujuan IT 188
10.3.2 Membuat IT Strategi yang Efektif 189
10.3.3 Mengembangkan Rencana Kerja IT yang jelas 189
10.3.4 Menilai dan Memilih teknologi yang tepat 190
10.4 Kebijakan dan Prosedur Keamanan 191
10.4.1 Membuat Kebijakan Keamanan IT 192
10.4.2 Mengembangkan Prosedur Keamanan Yang Efektif 192
10.5 Pengelolaan Identitas dan Akses 194
10.5.1 Mengelola Identitas dan Akses Pengguna 194
10.5.2 Menentukan Level Akses Yang Sesuai 195
10.5.3 Memastikan akses yang aman dengan otentikasi dan otorisasi yang tepat 196
10.5.4 Memonitor aktivitas pengguna 197
10.6 Keamanan Jaringan 198
10.6.1 Memastikan keamanan jaringan dengan firewall, VPN, dan teknologi keamanan jaringan lainnya 198
10.6.2 Membuat kebijakan keamanan jaringan yang jelas 199
10.6.3 Melindungi jaringan dari serangan dan ancaman keamanan 200
10.7 Pemulihan dan Penanganan Kejadian Keamanan 202
10.7.1 Menyiapkan Rencana Pemulihan Keamanan IT 202
10.7.2 Membuat prosedur untuk penanganan kejadian keamanan 203
10.7.3 Memonitor dan mengevaluasi penanganan kejadian keamanan 205
10.7.4 Meningkatkan sistem keamanan IT berdasarkan hasil evaluasi 205

DAFTAR PUSTAKA 207
BAB 11 KEBERLANGSUNGAN PERENCANAAN BISNIS 211
11.1 Pendahuluan 211
11.2 Pemahaman Tahap Keberlangsungan Perencanaan Bisnis 213
11.3 Pemahaman Proses Keberlangsungan Perencanaan Bisnis 219
11.3.1 Dampak Bisnis dan Analisis Risiko 221
11.3.2 Masalah Bangunan. 223
11.3.3 Masalah IT 225
11.3.4 Masalah Layanan Pelanggan 227
11.3.5 Masalah Teknis Operasional Administrasi 227
11.3.6 Masalah Pertanggungan Asuransi 228
11.3.7 Masalah Kepegawaian 228
11.3.8 Dokumen 229
11.3.9 Menangani Media 230
11.3.10 Biaya 230
11.3.11 Menguji, Mengaudit, Dan Terus Mengikuti Perkembangan 231
DAFTAR PUSTAKA 232
BAB 12 JAMINAN KUALITAS DAN STANDAR ASQ 233
12.1 Apakah Standar Kualitas itu? 233
12.2 Siapa yang Menggunakan Standar Kualitas 235
12.3 Mengapa Standar Penting? 236
12.3.1 Evaluasi kualitas untuk metodologi Model-Driven Web Engineering 237
12.3.2 Evaluasi Faktor Jaminan Kualitas dalam Metodologi Agile 237
12.3.3 Bagaimana meningkatkan penjaminan mutu perangkat lunak di negara-negara miskin 238

12.3.4 Standar & Spesifikasi Kualitas Konstruksi Soft-Scape di Malaysia 238
12.3.5 Menganalisis keefektifan dan ketergantungan sistem jaminan kualitas courseware E-learning 239
12.3.6 Jaminan Kualitas untuk Perangkat Lunak studi berdasarkan industri perangkat lunak di Pakistan 239
12.3.7 Metode Kuadrat Terkecil Logaritmik Fuzzy: Metodologi Proses Hierarki Analitik Grup Fuzzy untuk Manajemen Penjaminan Kualitas Perangkat Lunak 240
12.3.8 Implementasi dan Konfigurasi Model Manajemen Peningkatan Mutu Perguruan Tinggi 240
12.3.9 Menggunakan Model Kualitas ISO 9126 untuk menilai aplikasi bisnis-ke-bisnis 241
12.3.10 Framework dan aplikasi untuk mengintegrasikan RFID dengan sistem Quality Assurance 241
12.4 Mengapa Standar Dari ASQ? 242
12.5 Kesimpulan 242
DAFTAR PUSTAKA 244
BIODATA PENULIS

DAFTAR GAMBAR

Gambar 4.1. Contoh histogram penjualan barang dalam 1 tahun 60
Gambar 4.2. Contoh perbandingan penjualan barang dalam 2 tahun terakhir 61
Gambar 7.1. Tahapan Audit TI..... 135
Gambar 8.1. ITIL Service Lifecycle..... 147
Gambar 8.2. Service Value Chain ITIL 4..... 149
Gambar 9.1. Risiko dan Ketidakpastian..... 162
Gambar 9.2. Risk Breakdown Structure 163
Gambar 9.3. *IT Controll and Risk*..... 166
Gambar 9.4. *Model for corporate governance of ICT*..... 168
Gambar 9.5. *Domain APO 12 Managed Risk*..... 171
Gambar 12.1. Prinsip Standar Kualitas..... 234

DAFTAR TABEL

Tabel 4.1. Contoh Analisis Laporan Laba Rugi Komparatif 62
Tabel 4.2. Teknik sampling yang biasa digunakan..... 65
Tabel 4.3. Perintah ACL yang biasa digunakan dalam analisis data 71
Tabel 4.4. Kelebihan Dan Kekurangan Teknik Audit 81
Tabel 9.1. Aktivitas Pengumpulan Data..... 172
Tabel 9.2. Analisis Risiko..... 173
Tabel 9.3. Pertahankan profil risiko 175
Tabel 9.4. Mengartikulasikan risiko..... 176
Tabel 9.5. Mendefenisikan portofolio manajemen resiko..... 177
Tabel 9.6. Menanggapi Risiko..... 178
Tabel 11.1. Tiga Tahap Keberlangsungan 214

BAB 1
KONSEP DAN PENGENALAN IT AUDIT DAN KONTROL

Oleh Wahyuddin S

1.1 Pendahuluan

IT Audit atau Audit Teknologi Informasi adalah suatu kegiatan audit yang dilakukan untuk mengevaluasi dan menilai efektivitas, efisiensi, keamanan, dan ketersediaan sistem informasi dalam suatu organisasi. Tujuannya adalah untuk memastikan bahwa sistem informasi tersebut beroperasi dengan baik, memenuhi standar keamanan yang ditetapkan, dan mendukung tujuan bisnis organisasi. IT Audit biasanya dilakukan oleh seorang IT Auditor yang memiliki pengetahuan dan keterampilan dalam bidang teknologi informasi, audit, dan keamanan informasi. IT Auditor bertanggung jawab untuk mengidentifikasi risiko, menganalisis kelemahan dalam sistem informasi, dan memberikan rekomendasi untuk perbaikan.

Pada umumnya, IT Audit dilakukan secara periodik dan berkala untuk memastikan bahwa sistem informasi organisasi beroperasi dengan baik dan memenuhi standar keamanan yang ditetapkan. Audit ini dapat dilakukan secara internal oleh tim audit internal atau secara eksternal oleh pihak yang independen dan profesional.

IT Audit dapat melibatkan berbagai aspek seperti keamanan informasi, manajemen risiko, kepatuhan terhadap regulasi, performa sistem, dan pemulihan bencana. Hasil dari IT Audit dapat membantu manajemen dalam mengambil keputusan dan melakukan perbaikan untuk memastikan sistem

informasi organisasi beroperasi dengan baik, memenuhi standar keamanan, dan mendukung tujuan bisnis organisasi.

IT Audit dan kontrol merupakan dua hal yang erat terkait dalam pengelolaan sistem informasi suatu organisasi. IT Audit digunakan untuk mengevaluasi dan menilai efektivitas, efisiensi, keamanan, dan ketersediaan sistem informasi dalam organisasi, sedangkan kontrol digunakan untuk melindungi sistem informasi dari ancaman dan risiko yang mungkin terjadi. *Control* atau pengendalian dalam sistem informasi mencakup berbagai aspek, seperti pengendalian akses, pengendalian keamanan, pengendalian perubahan, pengendalian operasional, dan pengendalian pencegahan dan deteksi kecurangan. Control bertujuan untuk melindungi sistem informasi dari serangan atau risiko yang dapat mengganggu atau merusak sistem informasi tersebut.

IT Audit bertujuan untuk mengevaluasi efektivitas dan efisiensi control yang telah diterapkan dalam sistem informasi. Audit ini dilakukan untuk memastikan bahwa control yang telah diterapkan dapat berfungsi dengan baik dan mampu melindungi sistem informasi dari risiko dan ancaman yang mungkin terjadi.

Dalam melakukan IT Audit dan kontrol, beberapa hal yang perlu diperhatikan adalah:

1. Memahami tujuan dan lingkup audit dan kontrol yang akan dilakukan.
2. Mengidentifikasi risiko dan ancaman yang mungkin terjadi pada sistem informasi.
3. Melakukan evaluasi dan pengujian terhadap control yang telah diterapkan.
4. Memberikan rekomendasi dan tindakan perbaikan untuk meningkatkan efektivitas dan efisiensi control yang telah diterapkan.

Dalam kesimpulannya, IT Audit dan kontrol merupakan dua hal yang sangat penting dalam pengelolaan sistem informasi suatu organisasi. Control digunakan untuk melindungi sistem informasi dari ancaman dan risiko yang mungkin terjadi, sedangkan IT Audit digunakan untuk mengevaluasi efektivitas dan efisiensi control yang telah diterapkan dan memberikan rekomendasi untuk perbaikan (Sihotang *et al.,* 2023).

1.2 Konsep IT Audit

IT Audit atau Audit Teknologi Informasi merupakan suatu kegiatan audit yang bertujuan untuk mengevaluasi dan menilai efektivitas, efisiensi, keamanan, dan ketersediaan sistem informasi dalam suatu organisasi. Audit ini dilakukan untuk memastikan bahwa sistem informasi yang digunakan oleh organisasi beroperasi dengan baik, memenuhi standar keamanan, dan mendukung tujuan bisnis organisasi.

Dalam era digital seperti sekarang, keberadaan sistem informasi yang aman dan efektif sangatlah penting bagi organisasi. IT Audit membantu organisasi untuk memastikan bahwa sistem informasi yang digunakan sesuai dengan standar keamanan dan dapat diandalkan dalam mendukung kegiatan bisnis. IT Audit juga membantu organisasi untuk mengidentifikasi risiko-risiko yang mungkin terjadi pada sistem informasi dan memberikan rekomendasi untuk mengurangi risiko tersebut.

IT Audit dapat dilakukan oleh tim internal atau oleh pihak eksternal yang independen dan profesional. Tim internal dapat terdiri dari staf yang ditunjuk oleh manajemen untuk melakukan audit secara periodik. Sementara itu, pihak eksternal dapat terdiri dari firma audit yang memiliki keahlian khusus dalam bidang audit TI. Adapun tujuan dari IT Audit antara lain adalah untuk:

1. Memastikan keamanan dan ketersediaan data dalam sistem informasi.
2. Mengidentifikasi dan mengevaluasi risiko dalam sistem informasi.
3. Memastikan kepatuhan organisasi terhadap peraturan dan standar keamanan yang berlaku.
4. Memberikan rekomendasi untuk perbaikan dan pengembangan sistem informasi.
5. Meningkatkan efektivitas dan efisiensi operasional sistem informasi.

Dalam melakukan IT Audit, ada beberapa hal yang perlu diperhatikan, seperti memahami tujuan dan lingkup audit, mengidentifikasi risiko yang terkait dengan sistem informasi, melakukan pengujian dan analisis, dan memberikan rekomendasi untuk perbaikan. Dalam kesimpulannya, IT Audit merupakan kegiatan yang sangat penting untuk memastikan bahwa sistem informasi organisasi beroperasi dengan baik dan sesuai dengan standar keamanan yang ditetapkan. Audit ini membantu organisasi untuk mengidentifikasi risiko dan memberikan rekomendasi untuk mengurangi risiko tersebut (Muttaqin *et al.,* 2023; Santoso *et al.,* 2023).

1.3 Tipe IT Audit

Berikut adalah beberapa tipe IT Audit yang umum dilakukan:

1. *General Controls Review*
   Audit yang mengevaluasi kontrol umum dalam sistem informasi, seperti kebijakan dan prosedur, manajemen akses, manajemen perubahan, dan manajemen risiko.
2. *Application Control Review*
   Audit yang mengevaluasi kontrol aplikasi khusus, seperti kontrol input, proses, dan output dalam aplikasi.

3. *IT Governance Audit*
   Audit yang mengevaluasi struktur organisasi dan manajemen, serta pemenuhan kebijakan dan standar dalam teknologi informasi.
4. *Penetration Testing*
   Audit yang dilakukan dengan cara mencoba menembus keamanan sistem informasi dengan cara simulasi serangan.
5. *Compliance Audit*
   Audit yang mengevaluasi kepatuhan suatu organisasi terhadap peraturan dan standar tertentu, seperti PCI DSS, HIPAA, atau ISO 27001.
6. *Disaster Recovery and Business Continuity Planning Audit*:
   Audit yang mengevaluasi rencana pemulihan bencana dan kelangsungan bisnis dalam sistem informasi.
7. *Data Privacy Audit*
   Audit yang mengevaluasi kebijakan dan praktik privasi data dalam sistem informasi, termasuk perlindungan data pribadi dan kebijakan privasi GDPR dan CCPA (Tantriawan *et al.,* 2023).

1.4 Kategori Utama IT Audit

Berdasarkan spektrum Audit TI, ada tiga kategori utama dari audit TI, yaitu:

1. Audit Sistem
   Audit Sistem melibatkan pemeriksaan terhadap sistem informasi organisasi. Fokus audit ini adalah pada aspek teknis seperti infrastruktur TI, jaringan, database, aplikasi, sistem operasi, dan keamanan informasi. Tujuannya adalah untuk memastikan bahwa sistem informasi tersebut beroperasi dengan efektif dan efisien, meminimalkan risiko keamanan informasi, dan memenuhi standar keamanan yang ditetapkan.

2. Audit Proses Bisnis
   Audit Proses Bisnis melibatkan pemeriksaan terhadap proses bisnis yang terkait dengan penggunaan sistem informasi. Fokus audit ini adalah pada aspek non-teknis seperti kepatuhan terhadap regulasi, efisiensi, efektivitas, dan keandalan proses bisnis. Tujuannya adalah untuk memastikan bahwa proses bisnis yang terkait dengan penggunaan sistem informasi beroperasi dengan efektif dan efisien, memenuhi standar regulasi dan kebijakan yang berlaku, dan mendukung tujuan bisnis organisasi.
3. Audit Strategis
   Audit Strategis melibatkan pemeriksaan terhadap strategi dan arah kebijakan penggunaan TI dalam organisasi. Fokus audit ini adalah pada aspek strategis seperti keterkaitan antara penggunaan TI dengan tujuan bisnis organisasi, manajemen risiko TI, dan pengelolaan aset TI. Tujuannya adalah untuk memastikan bahwa penggunaan TI dalam organisasi telah dikembangkan dan dikelola secara efektif untuk mendukung tujuan bisnis organisasi, meminimalkan risiko, dan memastikan kepatuhan terhadap regulasi dan kebijakan yang berlaku(Wahyuddin, Rismayani, *et al.,* 2023).

1.5 Contoh Tipe IT Audit

Berikut adalah beberapa contoh dari tipe audit TI:

1. Audit Keamanan Sistem
   Audit ini bertujuan untuk menilai seberapa baik sistem TI dalam organisasi telah dilindungi dari ancaman keamanan dan risiko keamanan informasi yang mungkin terjadi. Pemeriksaan dilakukan pada aspek-aspek seperti keamanan jaringan, manajemen hak akses, sistem keamanan, dan pengelolaan identitas.

2. Audit Kepatuhan
   Audit ini bertujuan untuk menilai sejauh mana organisasi mematuhi regulasi dan kebijakan yang berlaku dalam penggunaan sistem TI. Contohnya adalah audit yang dilakukan untuk menilai apakah sebuah organisasi mematuhi standar-standar keamanan seperti ISO 27001 atau standar-standar privasi seperti GDPR.
3. Audit Performa TI
   Audit ini bertujuan untuk menilai efektivitas dan efisiensi dari penggunaan sistem TI dalam mencapai tujuan bisnis organisasi. Pemeriksaan dilakukan pada aspek-aspek seperti kecepatan sistem, ketersediaan sistem, penggunaan sumber daya, dan pengukuran kinerja.
4. Audit Pemulihan Bencana
   Audit ini bertujuan untuk menilai seberapa baik sistem TI organisasi dalam menghadapi dan memulihkan diri dari bencana seperti serangan siber atau bencana alam. Pemeriksaan dilakukan pada aspek-aspek seperti perencanaan pemulihan bencana, pengujian keandalan pemulihan bencana, dan kesiapan pengguna dalam menghadapi bencana.
5. Audit Manajemen Proyek TI
   Audit ini bertujuan untuk menilai seberapa baik proyek TI dalam organisasi telah dikelola dan dikendalikan. Pemeriksaan dilakukan pada aspek-aspek seperti perencanaan, pengendalian biaya dan jadwal, manajemen risiko, dan pengukuran kinerja proyek (Permana *et al.,* 2023).

1.6 Aplikasi IT Audit & Kontrol

Aplikasi IT Audit dan Kontrol dapat digunakan dalam berbagai aspek sistem informasi di dalam organisasi, seperti:

1. Pengelolaan risiko
   IT Audit dan Kontrol dapat membantu organisasi dalam mengidentifikasi, menilai, dan mengelola risiko yang terkait dengan sistem informasi mereka.
2. Pengendalian akses
   IT Audit dan Kontrol dapat membantu organisasi dalam mengendalikan akses ke sistem informasi mereka dengan mengatur tingkat akses dan hak akses pengguna.
3. Keamanan informasi
   IT Audit dan Kontrol dapat membantu organisasi dalam melindungi informasi penting dan rahasia dari ancaman dan serangan.
4. Pengelolaan perangkat keras dan perangkat lunak
   IT Audit dan Kontrol dapat membantu organisasi dalam mengelola dan memantau penggunaan perangkat keras dan perangkat lunak dalam sistem informasi mereka.
5. Keandalan dan integritas data
   IT Audit dan Kontrol dapat membantu organisasi dalam memastikan keandalan dan integritas data dalam sistem informasi mereka, termasuk menjaga konsistensi data dan mengurangi risiko kesalahan manusia.
6. Kepatuhan regulasi dan kebijakan
   IT Audit dan Kontrol dapat membantu organisasi dalam memastikan kepatuhan mereka terhadap regulasi dan kebijakan yang berlaku, termasuk standar keamanan dan privasi data.
7. Audit sistem
   IT Audit dan Kontrol dapat membantu organisasi dalam melakukan audit sistem untuk menilai efektivitas dan efisiensi sistem informasi mereka, serta untuk

mengidentifikasi area yang memerlukan perbaikan atau perbaikan.

8. Pemantauan dan pemeliharaan system
   IT Audit dan Kontrol dapat membantu organisasi dalam memantau dan memelihara sistem informasi mereka untuk memastikan ketersediaan dan keandalan sistem.

Dengan menerapkan aplikasi IT Audit dan Kontrol yang tepat, organisasi dapat memastikan bahwa sistem informasi mereka aman, efektif, dan efisien dalam memberikan layanan kepada pengguna. Selain itu, aplikasi ini juga dapat membantu organisasi dalam memenuhi regulasi dan kebijakan yang berlaku serta mengurangi risiko dan biaya yang terkait dengan sistem informasi (Wahyuddin, Sudipa, e*t al.,* 2023).

1.7 Framework COBIT 5

COBIT 5 (*Control Objectives for Information and Related Technology*) adalah kerangka kerja (*framework)* global yang dikembangkan oleh *Information Systems Audit and Control Association* (ISACA) dan *IT Governance Institute* (ITGI) untuk memastikan efektivitas dan efisiensi penggunaan teknologi informasi dalam organisasi. COBIT 5 membantu organisasi dalam pengelolaan risiko, pengendalian internal, dan memastikan keamanan informasi. COBIT 5 juga membantu organisasi dalam membangun dan mengelola arsitektur teknologi informasi yang terintegrasi dan efektif. COBIT 5 terdiri dari lima komponen utama yaitu:

1. Framework
   Berisi konsep dan prinsip-prinsip penting dalam pengelolaan teknologi informasi.

2. Process Reference Model
   Berisi deskripsi detail tentang proses-proses penting dalam pengelolaan teknologi informasi, termasuk deskripsi tujuan, aktivitas, dan tugas yang terkait.
3. Control Objectives
   Berisi tujuan pengendalian untuk setiap proses dalam Process Reference Model.
4. Management Guidelines
   Berisi panduan untuk membantu manajemen dalam memahami dan menerapkan COBIT 5 dalam organisasi.
5. Maturity Models
   Berisi alat untuk mengukur dan membandingkan tingkat kematangan organisasi dalam pengelolaan teknologi informasi.

COBIT 5 membantu organisasi dalam memastikan bahwa penggunaan teknologi informasi mendukung tujuan bisnis organisasi, meminimalkan risiko yang terkait dengan penggunaan teknologi informasi, memastikan kepatuhan terhadap regulasi dan kebijakan internal, serta meningkatkan efektivitas dan efisiensi dalam pengelolaan teknologi informasi (De Haes, Van Grembergen, & Debreceny, 2013).

DAFTAR PUSTAKA

De Haes, S., Van Grembergen, W., & Debreceny, R. S. 2013. COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307–324.

Muttaqin, M., Yuswardi, Y., Parewe, A. M. A. K., Ashari, I. F., Munsarif, M., Wahyuddin, S., … Gustiana, Z. 2023. *Pengantar Sistem Cerdas*. Yayasan Kita Menulis.

Permana, A. A., Wahyuddin, S., Santoso, L. W., Wibowo, G. W. N., Wardhani, A. K., Wahidin, A. J., … Wijayanti, R. R. 2023. *Machine Learning*. Global Eksekutif Teknologi.

Santoso, L. W., Fauzan, R., Kristiana, R., Puspita, S., Nugroho, J. W., & Wahyuddin, S. 2023. *Manajemen Sains*. Global Eksekutif Teknologi.

Sihotang, J. I., Arni, S., Darsin, D., Ashari, I. F., Siregar, M. N. H., Fadhillah, Y., … Wirapraja, A. 2023. *Kontrol dan Audit TI*. Yayasan Kita Menulis.

Tantriawan, H., Sasongko, D., Rizal, M., Lumbanraja, O. M., Suryani, S., Halid, A., … Sirwan, S. 2023. *Komunikasi Data dan Jaringan*. Yayasan Kita Menulis.

Wahyuddin, S., Rismayani, R., Sihotang, J. I., Aisa, S., Gunawan, H., Tamsir, N., … Harlina, S. 2023. *Data Warehouse dan Data Mining*. Yayasan Kita Menulis.

Wahyuddin, S., Sudipa, I. G. I., Putra, T. A. E., Wahidin, A. J., Syukrilla, W. A., Wardhani, A. K., … Santoso, L. W. 2023. *Data Mining*. Global Eksekutif Teknologi.

BAB 2
MEMBANGUN IT AUDIT INTERNAL YANG EFEKTIF

Oleh Nono Heryana

2.1 Pendahuluan

Bab 2 membahas tentang membangun IT Audit Internal yang efektif. Sebelum memulai pembahasan lebih lanjut, penting untuk memahami definisi IT Audit Internal dan manfaat dari IT Audit Internal yang efektif.

2.1.1 Definisi IT Audit Internal

IT Audit Internal adalah suatu proses penilaian yang dilakukan oleh auditor internal yang terkait dengan teknologi informasi (TI) yang dimiliki oleh sebuah organisasi, untuk menilai sejauh mana pengelolaan TI tersebut dapat mendukung tercapainya tujuan organisasi secara efektif dan efisien, serta memberikan jaminan atas keandalan, kerahasiaan, integritas, dan ketersediaan informasi yang dihasilkan oleh TI (Dewi, 2016).

IT Audit Internal dilakukan untuk memberikan keyakinan bahwa sistem informasi yang dimiliki oleh organisasi dapat diandalkan, dan dapat beroperasi sesuai dengan standar dan kebijakan yang telah ditetapkan. Audit dilakukan oleh tim internal yang terdiri dari auditor (Sihotang *et al,* 2023) yang memiliki pengetahuan dan keterampilan dalam bidang TI dan audit internal, sehingga dapat memberikan evaluasi yang independen dan obyektif terhadap pengelolaan TI organisasi.

Dalam membangun IT Audit Internal yang efektif (Suripatty, 2021), perlu memperhatikan beberapa hal, antara lain persiapan IT Audit Internal, pelaksanaan audit, pelaporan hasil audit, dan tindak lanjut atas rekomendasi audit. Persiapan IT Audit Internal mencakup pembentukan tim IT Audit Internal, pemahaman atas lingkup audit, penentuan sumber daya dan anggaran, serta pemilihan metodologi audit yang sesuai dengan tujuan audit (Pangarsa, 2021). Setelah persiapan dilakukan, pelaksanaan audit dilakukan dengan melakukan pemeriksaan dan pengujian atas sistem informasi yang ada dalam organisasi, dengan tujuan untuk mengevaluasi efektivitas dan efisiensi penggunaan TI serta pengendalian keamanan TI.

Pelaporan hasil audit dilakukan dengan menyajikan laporan audit yang berisi hasil temuan audit, rekomendasi, serta kesimpulan dan saran yang ditujukan kepada manajemen organisasi. Laporan audit ini dapat digunakan oleh manajemen dalam mengambil keputusan strategis terkait pengelolaan TI organisasi. Terakhir, tindak lanjut atas rekomendasi audit dilakukan untuk memastikan bahwa perbaikan dan perubahan yang diperlukan dapat dilakukan dengan tepat waktu dan efektif (Badewin & Melasari, 2023).

Dalam keseluruhan proses IT Audit Internal, auditor internal harus memastikan bahwa audit dilakukan secara independen dan objektif, serta mengikuti standar audit yang berlaku. Selain itu, auditor internal harus memiliki pengetahuan yang cukup dan *up-to-date* mengenai teknologi informasi dan audit internal untuk dapat melakukan audit secara efektif (Arethusa et al, 2022). Dengan memperhatikan hal-hal tersebut, maka organisasi dapat membangun IT Audit Internal yang efektif dan mendukung pengelolaan TI organisasi secara optimal.

2.1.2 Manfaat dari IT Audit Internal yang efektif

Manfaat dari IT Audit Internal yang efektif sangatlah penting bagi sebuah organisasi. IT Audit Internal yang efektif dapat membantu meningkatkan efektivitas, efisiensi, dan keandalan pengelolaan TI organisasi (Elisabeth, 2019). Selain itu, IT Audit Internal yang efektif juga dapat memberikan manfaat sebagai berikut:

1. Meningkatkan keamanan TI
2. Mencegah terjadinya fraud atau kecurangan dalam pengelolaan TI
3. Menjamin integritas, kerahasiaan, dan ketersediaan informasi yang dihasilkan oleh TI
4. Memberikan keyakinan dan jaminan bagi stakeholder mengenai keamanan TI
5. Meningkatkan kepercayaan publik dan reputasi organisasi
6. Mengidentifikasi risiko TI yang mungkin timbul dan memberikan rekomendasi untuk mengatasi risiko tersebut
7. Menunjukkan bahwa organisasi telah mematuhi peraturan dan standar yang berlaku.

Oleh karena itu, IT Audit Internal yang efektif sangatlah penting bagi sebuah organisasi untuk menjamin pengelolaan TI yang aman, andal, dan efektif.

2.2 Persiapan IT Audit Internal

Persiapan yang matang dan terstruktur dalam membangun IT Audit Internal yang efektif sangatlah penting. Persiapan meliputi pemilihan tim IT Audit Internal, pemahaman lingkup audit, penentuan sumber daya dan anggaran, serta pemilihan metodologi audit yang sesuai.

2.2.1 Membentuk Tim IT Audit Internal

Langkah pertama dalam mempersiapkan IT Audit Internal yang efektif adalah membentuk tim IT Audit Internal

yang terdiri dari auditor internal yang berkualitas dan memiliki kompetensi di bidang TI.

Dalam memilih anggota tim IT Audit Internal, organisasi harus memastikan bahwa kriteria yang digunakan untuk memilih anggota tim sudah jelas dan objektif. Kriteria tersebut menurut Muryani *et al* (2023) meliputi pendidikan, pengalaman, sertifikasi, kemampuan analisis, serta kemampuan komunikasi. Kriteria yang jelas dan objektif akan membantu organisasi untuk memilih anggota tim yang tepat, sehingga dapat meningkatkan efektivitas dan efisiensi audit.

Selain itu, tim IT Audit Internal harus memiliki kemampuan untuk memahami lingkungan TI organisasi dengan baik (Tumanggor & Adriansyah, 2020). Hal ini meliputi pemahaman atas sistem informasi yang ada, kebijakan dan prosedur pengelolaan TI yang berlaku, serta kontrol yang telah diterapkan oleh organisasi. Dengan memahami lingkungan TI organisasi dengan baik, tim IT Audit Internal dapat melakukan audit dengan lebih efektif dan efisien, serta dapat memberikan rekomendasi yang tepat kepada manajemen organisasi.

Selain kemampuan memahami lingkungan TI organisasi, tim IT Audit Internal juga harus mampu bekerja secara independen (Andriansyah, 2022). Hal ini penting agar audit dapat dilakukan secara objektif dan tidak dipengaruhi oleh faktor internal atau eksternal yang dapat memengaruhi hasil audit. Oleh karena itu, tim IT Audit Internal harus bekerja secara independen dan menghindari konflik kepentingan yang dapat memengaruhi kualitas audit.

Dalam keseluruhan proses pemilihan tim IT Audit Internal, organisasi harus memastikan bahwa anggota tim yang dipilih memiliki kemampuan yang cukup untuk melakukan audit internal dengan baik dan dapat mendukung tercapainya tujuan audit (Afwah & Nurwulan, 2022). Dengan demikian, organisasi dapat membangun tim IT Audit Internal yang efektif

dan dapat memberikan manfaat yang besar bagi pengelolaan TI organisasi.

2.2.2 Memahami Lingkup Audit

Dalam memahami lingkup audit, auditor internal harus memahami sistem dan infrastruktur TI yang ada di dalam organisasi. Hal ini meliputi pemahaman atas kebijakan, prosedur, serta kontrol yang telah diterapkan oleh organisasi untuk menjaga keamanan, integritas, dan ketersediaan data. Auditor internal harus memastikan bahwa kebijakan, prosedur, dan kontrol tersebut memadai dan efektif dalam melindungi aset TI organisasi.

Selain memahami sistem dan infrastruktur TI, auditor internal juga harus memahami karakteristik TI dan lingkungan bisnis di dalam organisasi. Setiap organisasi memiliki karakteristik dan kebutuhan bisnis yang berbeda-beda, sehingga auditor internal harus memahami lingkungan bisnis organisasi tersebut. Dengan memahami karakteristik TI dan lingkungan bisnis, auditor internal dapat menentukan pendekatan audit yang tepat dan memastikan bahwa audit dapat dilakukan secara efektif.

Auditor internal juga harus memahami standar dan regulasi yang berlaku terkait pengelolaan TI, seperti ISO 27001, COBIT, atau PCI DSS (Octariza, 2019). Hal ini akan membantu auditor internal dalam mengevaluasi kepatuhan organisasi terhadap standar dan regulasi yang berlaku, serta memberikan rekomendasi yang tepat kepada manajemen organisasi.

Dalam keseluruhan proses memahami lingkup audit, auditor internal harus memastikan bahwa audit dapat dilakukan dengan efektif dan sesuai dengan tujuan audit. Auditor internal harus memahami lingkup audit dengan baik, sehingga dapat mengevaluasi keamanan, integritas, dan

ketersediaan data dengan tepat dan memberikan rekomendasi yang tepat kepada manajemen organisasi.

2.2.3 Menentukan Sumber Daya dan Anggaran

Menentukan sumber daya dan anggaran yang cukup merupakan hal yang penting dalam pelaksanaan IT Audit Internal yang efektif. Sumber daya yang dimaksud meliputi sumber daya manusia, perangkat lunak, peralatan, dan sumber daya keuangan. Auditor internal harus memastikan bahwa sumber daya manusia yang dipilih memiliki kemampuan yang memadai dan memahami lingkup audit yang telah ditentukan. Selain itu, perangkat lunak dan peralatan yang digunakan harus memenuhi persyaratan teknis dan dapat mendukung pelaksanaan audit dengan efektif.

Penentuan anggaran harus mencakup biaya untuk persiapan, pelaksanaan, dan pelaporan hasil audit (Pane, 2022). Auditor internal harus memperkirakan biaya yang diperlukan dengan cermat agar tidak terjadi kekurangan dana di tengah-tengah pelaksanaan audit. Selain itu, auditor internal juga perlu menentukan alokasi anggaran yang tepat untuk setiap tahap audit, seperti persiapan, pengumpulan data, analisis, dan pelaporan hasil audit.

Dengan menentukan sumber daya dan anggaran yang cukup, auditor internal dapat memastikan bahwa audit dapat dilakukan dengan efektif dan hasil audit yang dihasilkan dapat memberikan nilai tambah yang signifikan bagi organisasi. Selain itu, penentuan sumber daya dan anggaran yang tepat juga dapat memastikan bahwa pelaksanaan audit berjalan lancar dan efisien tanpa adanya kendala yang signifikan.

2.2.4 Memilih Metodologi Audit yang Sesuai

Pemilihan metodologi audit yang tepat sangat penting untuk memastikan efektivitas dan efisiensi audit. *COBIT (Control Objectives for Information and related Technology)* adalah standar global untuk pengelolaan TI dan menjadi acuan utama untuk IT Audit Internal (Nugraha, 2017). COBIT membantu dalam mengidentifikasi dan menilai risiko TI dan memberikan panduan untuk mengimplementasikan kontrol dan tindakan perbaikan. Sedangkan *ITIL (Information Technology Infrastructure Library)* fokus pada pengelolaan layanan TI dan memberikan panduan untuk manajemen layanan TI berdasarkan proses (Gunawan, 2019). ITIL digunakan untuk menilai efektivitas layanan TI dan memberikan rekomendasi perbaikan. Sementara itu, *ISO 27001 (International Organization for Standardization)* adalah standar internasional untuk manajemen keamanan informasi yang meliputi aspek keamanan teknologi informasi, personil, dan proses (Chazar, 2015). ISO 27001 memberikan panduan untuk membangun sistem manajemen keamanan informasi yang efektif dan efisien (Rutanaji *et al*, 2017).

Dalam memilih metodologi audit yang sesuai, auditor internal juga harus mempertimbangkan karakteristik organisasi, seperti ukuran, kompleksitas, dan jenis industri yang dioperasikan. Misalnya, organisasi yang beroperasi di sektor keuangan akan memiliki kebutuhan audit TI yang berbeda dengan organisasi di sektor manufaktur. Auditor internal harus memahami karakteristik organisasi dan memilih metodologi audit yang dapat mengakomodasi kebutuhan audit TI yang spesifik.

2.3 Pemahaman Lingkungan TI Perusahaan

Pemahaman lingkungan TI perusahaan menjadi hal yang sangat penting dalam menjalankan IT audit internal yang efektif. Auditor internal harus memahami infrastruktur TI yang dimiliki perusahaan, termasuk sistem aplikasi dan proses bisnis yang digunakan. Pemahaman ini akan membantu auditor internal untuk menentukan risiko TI yang dapat mempengaruhi efektivitas pengelolaan TI perusahaan secara keseluruhan.

2.3.1 Evaluasi Infrastruktur TI

Evaluasi infrastruktur TI perusahaan oleh auditor internal juga meliputi penilaian terhadap perangkat lunak yang digunakan oleh perusahaan, termasuk sistem aplikasi yang mendukung operasi bisnis perusahaan. Auditor internal harus memeriksa kemampuan sistem aplikasi untuk memenuhi kebutuhan bisnis perusahaan serta keamanan dan privasi data yang tersimpan di dalamnya. Selain itu, auditor internal juga harus memastikan bahwa sistem aplikasi yang digunakan perusahaan sesuai dengan standar dan regulasi yang berlaku dalam industri (Sihotang, 2023).

Selain evaluasi infrastruktur TI dan sistem aplikasi, auditor internal juga harus memahami proses bisnis perusahaan secara menyeluruh. Auditor internal harus memahami bagaimana TI digunakan dalam mendukung proses bisnis dan memastikan bahwa sistem TI yang digunakan sesuai dengan kebutuhan bisnis. Auditor internal harus memeriksa penggunaan TI dalam berbagai fungsi bisnis, seperti produksi, pemasaran, keuangan, dan sumber daya manusia. Dengan pemahaman yang mendalam tentang proses bisnis perusahaan, auditor internal dapat menilai efektivitas pengelolaan TI dalam mendukung operasi bisnis perusahaan.

Dalam melaksanakan evaluasi infrastruktur TI perusahaan, analisis sistem aplikasi, dan pemahaman proses

bisnis perusahaan, auditor internal harus menggunakan metodologi audit yang tepat. Metodologi audit yang tepat akan memungkinkan auditor internal untuk menilai efektivitas pengelolaan TI secara holistik dan terintegrasi, mengidentifikasi risiko TI secara komprehensif, dan memberikan rekomendasi yang tepat untuk mengatasi risiko tersebut. Metodologi audit yang sering digunakan adalah COBIT, ITIL, dan ISO 27001.

2.3.2 Menganalisis Sistem Aplikasi yang Digunakan

Auditor internal harus memahami sistem aplikasi yang digunakan oleh perusahaan dan memeriksa keamanan sistem tersebut. Hal ini dapat dilakukan dengan melakukan analisis terhadap sistem aplikasi perusahaan, termasuk pemeriksaan kebijakan keamanan, penggunaan hak akses, dan kontrol yang diterapkan pada sistem tersebut. Auditor internal juga harus memeriksa kepatuhan sistem aplikasi dengan standar industri dan peraturan yang berlaku.

2.3.3 Memahami Proses Bisnis

Auditor internal harus memahami proses bisnis yang digunakan oleh perusahaan dalam menjalankan operasinya (Wulandari & Fidiana, 2017). Pemahaman ini penting untuk mengidentifikasi risiko TI yang dapat mempengaruhi efektivitas pengelolaan TI perusahaan. Auditor internal harus mengetahui bagaimana TI digunakan dalam mendukung operasi bisnis dan bagaimana risiko TI dapat mempengaruhi keberhasilan operasi bisnis tersebut. Selain itu, auditor internal juga harus memeriksa kepatuhan proses bisnis dengan standar industri dan peraturan yang berlaku.

2.4 Identifikasi Risiko TI

2.4.1 Melakukan Identifikasi Risiko

Identifikasi risiko TI merupakan tahapan penting dalam audit internal TI yang efektif (Amani et al, 2018). Pada tahapan ini, auditor internal harus melakukan identifikasi terhadap berbagai macam risiko TI yang dapat mempengaruhi efektivitas dan efisiensi pengelolaan TI organisasi.

Risiko TI dapat berasal dari berbagai faktor, seperti kebijakan dan prosedur yang lemah, ketidakmampuan untuk menangani serangan siber, kerentanan sistem dan jaringan, serta kurangnya pengelolaan hak akses pengguna. Auditor internal harus memastikan bahwa risiko TI telah diidentifikasi dengan benar dan akurat.

2.4.2 Mengklasifikasikan Risiko

Setelah melakukan identifikasi risiko, auditor internal perlu mengklasifikasikan risiko yang telah diidentifikasi. Klasifikasi risiko dapat dilakukan berdasarkan kriteria tertentu, seperti tingkat keparahan risiko, tingkat dampak risiko terhadap organisasi, atau prioritas risiko.

Dalam hal ini, auditor internal perlu mempertimbangkan klasifikasi risiko yang paling relevan dengan kebutuhan organisasi dan audit internal TI yang sedang dilakukan.

2.4.3 Menganalisis Dampak dan Kemungkinan Terjadinya Risiko

Setelah melakukan identifikasi dan klasifikasi risiko, auditor internal perlu menganalisis dampak dan kemungkinan terjadinya risiko (Aresteria, 2018). Analisis dampak risiko harus mencakup dampak yang dapat terjadi jika risiko terjadi, seperti kerugian finansial, reputasi yang buruk, atau kerugian operasional. Sementara itu, analisis kemungkinan terjadinya

risiko harus mencakup kemungkinan terjadinya risiko pada tingkat tertentu, seperti kemungkinan risiko terjadi dalam satu tahun atau lebih.

Dengan melakukan identifikasi, klasifikasi, dan analisis risiko TI, auditor internal dapat memberikan rekomendasi yang tepat untuk mengurangi atau menghilangkan risiko TI yang dapat mempengaruhi efektivitas dan efisiensi pengelolaan TI organisasi (Albone, 2009). Hal ini dapat membantu organisasi dalam meningkatkan pengelolaan TI yang lebih efektif dan efisien, serta meningkatkan keamanan, integritas, dan ketersediaan data.

2.5 Penetapan Prioritas dan Rencana Audit

2.5.1 Menentukan Prioritas Risiko

Setelah mengidentifikasi risiko, auditor internal harus memprioritaskan risiko-risiko tersebut. Hal ini akan membantu auditor internal dalam menentukan tindakan yang harus dilakukan untuk mengurangi atau menghilangkan risiko yang telah diidentifikasi. Prioritas risiko ditentukan berdasarkan tingkat dampak dan kemungkinan terjadinya risiko (Rahmawati & Wijaya, 2019). Risiko-risiko yang memiliki dampak besar dan kemungkinan terjadinya tinggi harus dianggap sebagai prioritas utama untuk ditangani terlebih dahulu. Dengan memprioritaskan risiko, perusahaan dapat mengalokasikan sumber daya yang terbatas dengan lebih efektif untuk mengatasi risiko-risiko yang paling signifikan dan dapat mempengaruhi operasi bisnis perusahaan secara signifikan.

Menentukan prioritas risiko juga membantu auditor internal dalam menentukan strategi penanganan risiko. Risiko-risiko yang memiliki prioritas tinggi akan memerlukan strategi penanganan risiko yang lebih proaktif dan efektif. Sementara risiko-risiko yang memiliki dampak kecil dan kemungkinan

terjadinya rendah dapat diatasi dengan strategi yang lebih sederhana atau bahkan tidak memerlukan tindakan khusus. Dengan menentukan prioritas risiko secara tepat, perusahaan dapat memaksimalkan manfaat dari audit internal TI dan memastikan bahwa sumber daya yang digunakan untuk mengatasi risiko dilakukan dengan efektif.

2.5.2 Menentukan Rencana Audit

Setelah menentukan prioritas risiko, auditor internal harus menentukan rencana audit (Nugrahini, 2015). Rencana audit mencakup jadwal, sumber daya, dan metode yang akan digunakan untuk melakukan audit.

Rencana audit harus disusun dengan mempertimbangkan sumber daya yang tersedia, tingkat prioritas risiko, dan tujuan audit. Rencana audit harus mencakup pemeriksaan kebijakan, prosedur, kontrol, dan infrastruktur TI yang berkaitan dengan risiko yang telah diidentifikasi. Selain itu, rencana audit juga harus memperhatikan regulasi dan standar yang berlaku di bidang TI dan keamanan informasi.

2.6 Pelaksanaan Audit

Pelaksanaan audit merupakan tahap yang sangat penting dalam proses IT Audit Internal. Pada tahap ini, auditor internal akan melakukan audit terhadap sistem dan infrastruktur TI yang telah diidentifikasi risikonya pada tahap sebelumnya.

2.6.1 Melakukan Audit

Pada tahap ini, auditor internal akan melaksanakan rencana audit yang telah ditetapkan pada tahap sebelumnya. Auditor internal akan mengumpulkan bukti-bukti dan informasi yang diperlukan melalui wawancara dengan pihak-pihak terkait dan pemeriksaan dokumen. Selama pelaksanaan

audit, auditor internal harus memastikan bahwa mereka menjalankan audit secara independen dan objektif.

2.6.2 Mengevaluasi Keamanan Sistem

Dalam pelaksanaan audit, evaluasi keamanan sistem menjadi hal yang sangat penting (Gusman et *al*, 2021). Auditor internal akan melakukan penilaian terhadap kebijakan keamanan yang telah diterapkan dan mengecek apakah infrastruktur dan sistem TI perusahaan sudah cukup aman. Auditor internal juga akan mengevaluasi penggunaan sandi dan kebijakan akses, serta memeriksa apakah penggunaannya sudah sesuai dengan standar keamanan yang berlaku.

Dalam melakukan evaluasi keamanan sistem, auditor internal juga akan memperhatikan segala bentuk ancaman yang dapat terjadi, termasuk ancaman dari luar maupun dari dalam perusahaan. Auditor internal harus memastikan bahwa segala kebijakan keamanan TI yang diterapkan sudah mampu mengatasi segala bentuk ancaman tersebut. Selain itu, auditor internal juga harus memeriksa apakah perusahaan sudah menerapkan sistem deteksi dan respons cepat yang efektif dalam mengatasi ancaman keamanan TI yang mungkin terjadi.

2.6.3 Mengevaluasi Pengelolaan Data

Pada tahap ini, auditor internal akan mengevaluasi pengelolaan data organisasi, termasuk kebijakan penyimpanan data, backup dan recovery, serta integritas data. Auditor internal juga akan memeriksa apakah data tersebut diakses dan digunakan secara sah dan apakah dilakukan dengan standar keamanan yang telah ditetapkan.

2.6.4 Melakukan Pengujian Aplikasi

Pada tahap ini, auditor internal akan melakukan pengujian aplikasi untuk memastikan bahwa aplikasi tersebut berfungsi sesuai dengan yang diharapkan dan sesuai dengan standar keamanan dan kualitas yang telah ditetapkan. Auditor internal akan memeriksa apakah pengujian yang dilakukan telah dilakukan secara menyeluruh dan akurat, serta melakukan evaluasi terhadap hasil pengujian tersebut.

Setelah tahap pelaksanaan audit selesai, auditor internal akan mengumpulkan semua bukti-bukti dan informasi yang diperoleh selama pelaksanaan audit untuk dilaporkan pada tahap berikutnya.

2.7 Pelaporan Hasil Audit

2.7.1 Membuat Laporan Hasil Audit

Setelah audit selesai dilakukan, auditor internal harus membuat laporan hasil audit yang berisi temuan-temuan dan rekomendasi yang disampaikan kepada manajemen.

Laporan hasil audit harus dibuat secara obyektif dan profesional (Nurjanah & Kartika, 2016) dengan mempertimbangkan keseluruhan fakta dan bukti yang didapat selama audit. Laporan hasil audit harus mencakup analisis atas risiko yang ditemukan, rekomendasi untuk mengatasi risiko, serta kesimpulan dan rekomendasi untuk perbaikan sistem dan infrastruktur TI.

2.7.2 Menyampaikan Laporan Hasil Audit

Setelah laporan hasil audit selesai dibuat, auditor internal harus menyampaikan laporan tersebut kepada manajemen perusahaan. Pelaporan harus dilakukan dengan cara yang jelas dan mudah dipahami oleh manajemen. Selain itu, auditor internal juga harus menjelaskan secara rinci

mengenai temuan-temuan dan rekomendasi yang diberikan dalam laporan hasil audit.

2.7.3 Menentukan Tindak Lanjut dari Hasil Audit

Setelah laporan hasil audit disampaikan, manajemen perusahaan harus menentukan tindak lanjut dari hasil audit tersebut. Tindak lanjut tersebut dapat berupa perbaikan sistem dan infrastruktur TI, pemberian pelatihan kepada karyawan, atau perbaikan kebijakan dan prosedur.

Tindak lanjut dari hasil audit harus direncanakan dan dilaksanakan sesegera mungkin agar risiko-risiko yang ditemukan dapat diminimalisir. Auditor internal harus memonitor tindak lanjut dari hasil audit untuk memastikan bahwa tindak lanjut tersebut efektif dan efisien.

2.8 Monitoring dan Evaluasi

2.8.1 Menentukan Program Monitoring dan Evaluasi

Setelah audit internal TI selesai dilakukan, langkah selanjutnya adalah menentukan program monitoring dan evaluasi yang bertujuan untuk memastikan bahwa tindakan yang diambil untuk mengatasi temuan audit telah dilaksanakan dengan efektif dan efisien.

Program monitoring dan evaluasi harus mencakup indikator kinerja dan target yang jelas, serta mekanisme pengumpulan dan analisis data yang dapat digunakan untuk mengukur tingkat keberhasilan program.

2.8.2 Menilai Efektivitas Audit Internal TI

Penilaian efektivitas audit internal TI harus dilakukan secara teratur untuk memastikan bahwa audit internal TI berjalan sesuai dengan rencana, serta untuk mengevaluasi hasil yang telah dicapai.

Hal ini dapat dilakukan dengan membandingkan hasil audit dengan rencana audit, serta melakukan wawancara dengan karyawan dan manajemen untuk mendapatkan masukan dan umpan balik tentang proses audit.

2.8.3 Memperbaiki Proses Audit Internal TI

Hasil evaluasi audit internal TI akan menjadi dasar untuk melakukan perbaikan dan peningkatan proses audit internal TI secara terus-menerus (Amani, 2018). Hal ini dilakukan agar proses audit dapat berjalan lebih efektif dan efisien, serta menghasilkan hasil audit yang lebih akurat dan relevan. Perbaikan dapat dilakukan dengan memperbarui metodologi audit internal TI yang digunakan dan mengikuti perkembangan teknologi terkini, sehingga audit dapat dilakukan secara lebih efektif. Selain itu, memberikan pelatihan kepada tim audit internal TI juga menjadi salah satu cara untuk meningkatkan kemampuan mereka dalam melakukan audit internal TI dengan lebih efektif dan efisien.

Setelah melakukan perbaikan dan peningkatan proses audit internal TI, perusahaan perlu melakukan evaluasi ulang terhadap hasil audit yang telah dilakukan. Evaluasi ulang ini dilakukan untuk memastikan bahwa perbaikan dan peningkatan yang dilakukan dapat memberikan manfaat dan memberikan dampak yang signifikan terhadap efektivitas pengelolaan TI perusahaan. Dengan melakukan evaluasi ulang secara berkala, perusahaan dapat memastikan bahwa proses audit internal TI dapat berjalan dengan baik dan menghasilkan hasil yang akurat dan relevan bagi perusahaan.

DAFTAR PUSTAKA

AFWAH, S. N., & Nurwulan, L. L. 2022. Pengaruh Komite Audit, Kompetensi Auditor Internal Dan Efektivitas Pengendalian Internal Terhadap Pencegahan Kecurangan (Fraud)(Studi Pada PT Pos Indonesia Persero) (Doctoral dissertation, Fakultas Ekonomi dan Bisnis).

AlBone, A. 2009. Pembuatan rencana keamanan informasi berdasarkan Analisis dan mitigasi risiko teknologi informasi. Jurnal Informatika, 10(1), 44-52.

Amani, T., Vidiyastutik, E. D., & Hudzafidah, K. 2018. Dampak Teknologi Informasi Terhadap Audit Internal. UNEJ e-Proceeding, 58-66.

Andriansyah, M. 2020. Pengaruh Akuntabilitas Dan Independensi Auditor Terhadap Kualitas Audit (Studi Kasus Pada Kantor Akuntan Publik Di Bekasi) (Doctoral dissertation, Sekolah Tinggi Ilmu Ekonomi Indonesia Jakarta).

Aresteria, M. 2018. Peran Audit Internal Dalam Pencegahan Fraud di Perguruan Tinggi: Literature Review. Jurnal Akuntansi, Ekonomi dan Manajemen Bisnis, 6(1), 45-53.

Arethusa, A. F., Oktaroza, M. L., & Maemunah, M. 2022, July. Pengaruh Kompetensi Auditor dan Implementasi e-Audit terhadap Kualitas Audit. In Bandung Conference Series: Accountancy (Vol. 2, No. 2, pp. 1145-1151).

Badewin, S. E., & Ranti Melasari, S. E. 2023. AUDIT MANAJEMEN PETUNJUK BAGI PRAKTISI. Uwais Inspirasi Indonesia.

Chazar, C. 2015. Standar manajemen keamanan sistem informasi berbasis ISO/IEC 27001: 2005. Jurnal Informatika dan Sistem Informasi, 7(2), 48-57.

Dewi, R. A. 2016. Pengaruh Peran, Profesionalisme, Pengalaman Kerja, Dan Pengetahuan Information Technology (It) Auditor Internal Terhadap Efektivitas Sistem Pengendalian Internal Perusahaan (Bachelor's thesis, Jakarta: Fakultas Ekonomi dan Bisnis UIN Syarif Hidayatullah Jakarta).

Elisabeth, D. M. 2019. Kajian terhadap peranan teknologi informasi dalam perkembangan audit komputerisasi (studi kajian teoritis). METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi, 3(1), 40-53.

Gunawan, H. 2019. Desain Model Manajemen Layanan TI berbasis Information Technology Infrastructure Library (ITIL). MEANS (Media Informasi Analisa dan Sistem), 104-111.

Gusman, D. V., Prasetyo, F. H., & Adi, K. 2021. Audit Sistem Keamanan TI Menggunakan Domain DSS05 Pada Framework COBIT 5 (Studi Kasus: Diskominfo Kabupaten Karawang). Jurnal Informatika Upgris, 7(1).

Muryani, E., Sulistiarini, E. B., Prihatiningsih, T. S., Ramadhana, M. R., Heriteluna, M., Maghfur, I., ... & Purnomo, A. 2022. Manajemen Sumber Daya Manusia. UNISMA PRESS.

Nugraha, B. 2017. Analisis dan Evaluasi Sistem Informasi Akademik Menggunakan COBIT@ 5 PAM (Process Assesment Model)(Studi Kasus Pada Universitas Singaperbangsa Karawang). SYNTAX, 6(1), 47-56.

Nugrahini, P. 2015. Pengaruh kompetensi dan profesionalisme auditor Internal terhadap kualitas audit (Studi Empiris pada BUMN dan BUMD di Kota Yogyakarta). Skripsi Fakultas Ekonomi Universitas Negeri Yogyakarta.

Nurjanah, I. B., & Kartika, A. 2016. Pengaruh kompetensi, independensi, etika, pengalaman auditor, skeptisme profesional auditor, objektifitas dan integritas terhadap kualitas audit (Studi pada Kantor Akuntan Publik di Kota Semarang). Dinamika Akuntansi Keuangan dan Perbankan, 5(2).

Octariza, N. F. 2019. Analisis sistem manajemen keamanan informasi menggunakan standar iso/Iec 27001 dan iso/lec 27002 pada kantor pusat pt jasa mar (Bachelor's thesis, Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta).

Pane, F. L. S. S. 2022. Peran internal auditor dalam pemeriksaan kredit pada PT. Bank Sumut Cabang Koordinator Medan (Doctoral dissertation).

Pangarsa, B. A. 2021. Audit Internal Berbasis Risiko Bidang Perkreditan di Bank X (Doctoral dissertation).

Rahmawati, A., & Wijaya, A. F. 2019. Analisis risiko teknologi informasi menggunakan ISO 31000 pada Aplikasi ITOP. Jurnal SITECH: Sistem Informasi dan Teknologi, 2(1), 13-20.

Rutanaji, D., Kusumawardani, S. S., & Winarno, W. W. 2017. ISO 27001 sebagai Metode Alternatif bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan untuk Diterapkan di Arsip Nasional RI). ReTII.

Sihotang, J. I., Arni, S., Darsin, D., Ashari, I. F., Siregar, M. N. H., Fadhillah, Y., ... & Yuniwati, I. 2023. Kontrol dan Audit TI. Yayasan Kita Menulis.

Suripatty, R. 2021. Peran Audit Internal Dalam Mewujudkan Good Corpoorate Governance Pada Kantor Pengawasan Dan Pelayanan Bea Cukai (Kppbc) Kota Sorong Propinsi Papua Barat. PELUANG, 15(1).

Tumanggor, A. H., & Adriansyah, T. M. 2020. Dampak Teknologi Informasi Terhadap Audit Internal. Juripol (Jurnal Institusi Politeknik Ganesha Medan), 3(2), 105-115.

Wulandari, T., & Fidiana, F. 2017. Peranan Audit Internal Terhadap Kepatuhan Standar Operasional Prosedur (SOP) Pada PT X. Jurnal Ilmu dan Riset Akuntansi (JIRA), 6(7).

BAB 3
METODE DAN PROSES AUDIT TEKNOLOGI INFORMASI

Oleh Alexander Waworuntu

3.1 Pendahuluan

Di era digital saat ini, organisasi lintas industri mengandalkan teknologi informasi (TI) untuk mendorong operasi mereka, pengambilan keputusan strategis, dan kesuksesan bisnis secara keseluruhan. Karena kompleksitas dan ketergantungan pada sistem TI terus meningkat, demikian pula risiko yang terkait dengan potensi pelanggaran keamanan, kehilangan data, dan pelanggaran kepatuhan. Akibatnya, audit TI telah menjadi alat penting bagi organisasi untuk menilai, mengevaluasi, dan mengelola lingkungan TI mereka secara efektif (Hall, 2015).

Metode dan proses audit TI memberikan pendekatan sistematis bagi organisasi untuk mengidentifikasi, mengevaluasi, dan mengurangi risiko yang terkait dengan infrastruktur, kebijakan, dan operasi TI mereka. Dengan mengikuti metodologi terstruktur, auditor TI dapat memastikan kerahasiaan, integritas, dan ketersediaan aset informasi sekaligus mempromosikan kepatuhan terhadap persyaratan peraturan, standar industri, dan kebijakan internal. Selain itu, audit TI membantu organisasi meningkatkan tata kelola TI mereka, mengoptimalkan alokasi sumber daya, dan menumbuhkan budaya peningkatan dan akuntabilitas berkelanjutan (Merhout and Havelka, 2008).

3.2 Tujuan Audit TI

Dalam aktivitas audit TI apa pun, tujuan audit harus selaras dengan tujuan bisnis dari area atau proses yang sedang ditinjau. Dengan berfokus pada risiko dan kontrol penting yang dapat berdampak pada pencapaian tujuan ini, auditor dapat memberikan wawasan dan rekomendasi yang berharga untuk meningkatkan lingkungan TI organisasi. Memastikan bahwa tujuan audit konsisten dengan tujuan organisasi yang lebih luas membantu auditor memberikan hasil yang berarti dan mendorong kesuksesan bisnis (Senft, Gallegos and Davis, 2012). Berikut adalah lima bidang utama di mana tujuan audit harus selaras dengan tujuan organisasi:

1. **Pencapaian Sasaran dan Sasaran Operasional**
   Audit TI harus mengevaluasi sejauh mana sistem dan proses TI mendukung pencapaian tujuan dan sasaran operasional organisasi. Ini mungkin termasuk menilai kinerja, keandalan, dan skalabilitas sistem TI, serta kemampuannya untuk mendukung inisiatif strategis, seperti transformasi digital, otomatisasi proses, dan analitik data. Dengan mengidentifikasi potensi kemacetan, inefisiensi, dan kerentanan dalam operasi TI, auditor dapat membantu organisasi mengoptimalkan infrastruktur dan proses TI mereka untuk mencapai tujuan operasional mereka.
2. **Keandalan dan Integritas Informasi**
   Informasi yang akurat, tepat waktu, dan andal sangat penting untuk pengambilan keputusan, pelaporan, dan kepatuhan. Auditor TI harus menilai kontrol dan proses yang ada untuk memastikan keandalan dan integritas informasi organisasi. Ini mungkin melibatkan evaluasi kelengkapan, akurasi, dan ketepatan waktu input, pemrosesan, dan output data, serta efektivitas praktik manajemen kualitas data. Dengan mengidentifikasi dan

mengatasi masalah yang dapat memengaruhi keandalan dan integritas informasi, auditor dapat membantu organisasi membuat keputusan berdasarkan informasi yang lebih baik dan mempertahankan kepercayaan pemangku kepentingan.

3. **Pengamanan Aset**
   Organisasi harus melindungi aset TI penting mereka, termasuk perangkat keras, perangkat lunak, dan data, dari akses tidak sah, pencurian, kerusakan, atau kehilangan. Auditor TI harus menilai kontrol dan proses yang ada untuk melindungi aset ini, seperti tindakan keamanan fisik, kontrol akses, teknik enkripsi, dan mekanisme pencadangan dan pemulihan. Dengan mengidentifikasi potensi kerentanan dan celah dalam tindakan perlindungan aset organisasi, auditor dapat membantu memperkuat postur keamanan organisasi secara keseluruhan dan menjaga aset TI yang berharga.
4. **Penggunaan Sumber Daya yang Efektif dan Efisien**
   Mengoptimalkan penggunaan sumber daya TI, seperti perangkat keras, perangkat lunak, dan personel, sangat penting bagi organisasi untuk mengendalikan biaya, meningkatkan produktivitas, dan mencapai keunggulan kompetitif. Auditor TI harus mengevaluasi alokasi, pemanfaatan, dan praktik manajemen sumber daya TI organisasi untuk memastikan mereka mendukung penggunaan sumber daya yang efektif dan efisien. Ini mungkin termasuk penilaian kesesuaian investasi TI, keselarasan alokasi sumber daya TI dengan prioritas bisnis, dan efektivitas proses manajemen sumber daya TI, seperti perencanaan kapasitas, manajemen aset, dan manajemen vendor. Dengan mengidentifikasi peluang untuk meningkatkan pemanfaatan dan pengelolaan sumber daya TI organisasi, auditor dapat membantu mendorong

penghematan biaya dan meningkatkan efisiensi operasional.

5. **Kepatuhan terhadap Kebijakan, Prosedur, Hukum, dan Peraturan Penting**
   Audit TI harus memastikan bahwa lingkungan TI organisasi mematuhi kebijakan dan prosedur internal yang relevan, serta hukum dan peraturan eksternal. Ketidakpatuhan dapat mengakibatkan penalti finansial yang signifikan, kerusakan reputasi, dan hilangnya peluang bisnis. Auditor TI harus menilai sistem dan proses TI organisasi untuk kepatuhan terhadap persyaratan yang berlaku, seperti undang-undang perlindungan data, peraturan khusus industri, dan standar pelaporan keuangan. Mereka juga harus mengevaluasi kebijakan dan prosedur TI internal organisasi untuk memastikannya mutakhir, komprehensif, dan dikomunikasikan secara efektif kepada karyawan. Dengan mengidentifikasi area ketidakpatuhan dan merekomendasikan perbaikan, auditor dapat membantu organisasi meminimalkan paparan hukum dan peraturan mereka, menghindari penalti yang mahal, dan mempertahankan reputasi yang kuat di pasar.

Menyelaraskan tujuan audit TI dengan tujuan bisnis organisasi yang lebih luas sangat penting untuk memberikan hasil yang berarti dan mendorong kesuksesan bisnis. Dengan berfokus pada area yang memiliki dampak terbesar pada tujuan operasional organisasi, keandalan informasi, pengamanan aset, optimalisasi sumber daya, dan kepatuhan, auditor TI dapat memberikan wawasan dan rekomendasi berharga untuk meningkatkan lingkungan TI organisasi, memitigasi risiko, dan mendukung pencapaian. dari tujuan strategisnya. Penyelarasan ini memastikan bahwa audit TI

berkontribusi pada keseluruhan kinerja, ketahanan, dan daya saing organisasi di dunia yang semakin digital.

3.3 Metodologi Audit TI

Metodologi audit TI adalah pendekatan terstruktur untuk mengevaluasi dan menilai infrastruktur, proses, dan kontrol teknologi informasi (TI) organisasi (Ackerman *et al.*, 2009). Ini bertujuan untuk memastikan bahwa sistem TI aman, andal, dan beroperasi secara efisien sesuai dengan undang-undang, peraturan, dan praktik terbaik yang berlaku (Otero, 2018). Metodologi ini terdiri dari beberapa fase utama, yaitu: Perencanaan (*Planning*), Penilaian Resiko (*Risk Assesment*), Evaluasi Kontrol (*Control Evaluation*), Pengujian (*Testing*), Pelaporan (*Reporting*), dan Tindak Lanjut (*Follow-up*).

3.3.1 Perencanaan (*Planning*)

Perencanaan adalah langkah penting dalam keseluruhan proses audit TI, karena menetapkan dasar untuk audit yang berhasil. Fase ini dijabarkan lebih lanjut di bawah ini:

1. **Memahami tujuan organisasi dan lingkungan TI:**
   Sebelum memulai audit, penting untuk mendapatkan pemahaman mendalam tentang tujuan bisnis organisasi, operasi, dan bagaimana lingkungan TI mendukung tujuan tersebut. Ini termasuk memahami industri organisasi, persyaratan peraturan, struktur organisasi, infrastruktur TI, dan aplikasi utama. Pengetahuan ini membantu auditor memfokuskan upaya mereka pada area dengan risiko lebih tinggi dan relevansi dengan organisasi.
2. **Mengidentifikasi ruang lingkup dan tujuan audit:**
   Ruang lingkup audit menentukan batasan dan bidang khusus yang akan diperiksa, sedangkan tujuan menguraikan hasil dan tujuan audit yang diharapkan. Ruang lingkup dan tujuan harus diselaraskan dengan selera risiko organisasi, tujuan strategis, dan persyaratan peraturan.

Auditor harus memastikan bahwa ruang lingkup dan tujuan didefinisikan dengan jelas dan disepakati oleh pemangku kepentingan terkait, termasuk manajemen dan komite audit.

3. **Memilih kriteria audit:**
   Kriteria audit adalah tolok ukur atau standar terhadap mana sistem, proses, dan kontrol TI organisasi akan dievaluasi. Kriteria ini dapat mencakup praktik terbaik industri, persyaratan peraturan, serta kebijakan dan prosedur internal. Auditor harus memilih kriteria yang tepat untuk memastikan penilaian yang komprehensif terhadap lingkungan TI organisasi.
4. **Mengembangkan rencana audit:**
   Rencana audit adalah dokumen terperinci yang menguraikan pendekatan, prosedur, dan kegiatan yang akan dilakukan selama audit. Rencana tersebut harus mencakup elemen-elemen berikut:
   - Ruang lingkup dan tujuan audit
   - Sumber daya yang diperlukan, termasuk ukuran dan keahlian tim audit
   - Garis waktu, termasuk tonggak penting dan tenggat waktu
   - Metodologi penilaian risiko
   - Prosedur dan teknik pengujian
   - Protokol pelaporan dan komunikasi
5. **Mendefinisikan peran dan tanggung jawab tim audit:**
   Mendefinisikan dengan jelas peran dan tanggung jawab anggota tim audit sangat penting untuk keberhasilan audit. Hal ini membantu memastikan bahwa setiap anggota tim memahami tugas, harapan, dan tingkat wewenang mereka dalam audit. Peran tersebut dapat mencakup auditor TI, pakar materi pelajaran, dan staf pendukung, masing-masing dengan tanggung jawab dan keahlian unik mereka.

Perencanaan Audit TI adalah fase kritis yang menentukan tahapan untuk audit TI yang sukses. Ini melibatkan pemahaman tujuan organisasi dan lingkungan TI, menentukan ruang lingkup dan tujuan audit, memilih kriteria audit yang sesuai, mengembangkan rencana audit yang komprehensif, dan menugaskan peran dan tanggung jawab kepada anggota tim audit. Pendekatan terstruktur ini membantu memastikan bahwa audit dilakukan secara efisien, efektif, dan selaras dengan kebutuhan dan prioritas organisasi.

3.3.2 Penilaian Resiko (*Risk Assessment*)

Penilaian Risiko membantu auditor memfokuskan upaya mereka pada risiko paling signifikan yang dihadapi organisasi (Stoneburner, Goguen and Feringa, 2002). Fase ini dapat dijabarkan sebagai berikut:

1. **Mengidentifikasi potensi risiko:**
   Langkah pertama dalam proses penilaian risiko adalah mengidentifikasi potensi risiko yang dapat memengaruhi sistem, proses, dan kontrol TI organisasi. Risiko ini dapat timbul dari berbagai sumber, seperti kegagalan teknologi, kesalahan manusia, ancaman keamanan, ketidakpatuhan terhadap peraturan, atau bencana alam. Auditor harus mempertimbangkan faktor internal dan eksternal saat mengidentifikasi risiko.
2. **Menilai kemungkinan dan dampak risiko:**
   Setelah potensi risiko diidentifikasi, auditor menilai kemungkinan terjadinya setiap risiko dan potensi dampaknya terhadap organisasi jika hal itu terjadi. Kemungkinan mengacu pada kemungkinan terjadinya peristiwa risiko, sedangkan dampak mengacu pada potensi konsekuensi atau kerusakan yang dapat ditimbulkan oleh peristiwa tersebut terhadap organisasi. Kemungkinan dan dampak harus dinilai menggunakan metode kualitatif

dan/atau kuantitatif, seperti penilaian ahli, data historis, atau model risiko.

3. **Memprioritaskan risiko:**
   Setelah menilai kemungkinan dan dampak dari setiap risiko, auditor memprioritaskan risiko berdasarkan signifikansinya bagi organisasi. Prioritas ini membantu auditor mengalokasikan sumber daya dan memfokuskan upaya mereka pada area dengan potensi dampak tertinggi. Metode umum untuk memprioritaskan risiko meliputi matriks risiko, peta panas risiko, atau sistem penilaian risiko.
4. **Memetakan risiko ke kontrol TI:**
   Setelah risiko diprioritaskan, auditor memetakannya ke kontrol, proses, atau sistem TI yang relevan. Hal ini membantu untuk menentukan keefektifan pengendalian yang ada dalam memitigasi risiko dan mengidentifikasi setiap celah pengendalian yang mungkin perlu ditangani.
5. **Mempertimbangkan faktor organisasi:**
   Penilaian risiko harus mempertimbangkan faktor unik organisasi, seperti ukuran, kompleksitas, industri, lingkungan peraturan, dan selera risiko. Faktor-faktor ini dapat memengaruhi kemungkinan dan dampak risiko, serta kemampuan organisasi untuk menanggapi dan mengelola risiko secara efektif.
6. **Mendokumentasikan penilaian risiko:**
   Hasil penilaian risiko harus didokumentasikan secara jelas, ringkas, dan konsisten. Dokumentasi ini harus mencakup risiko yang teridentifikasi, kemungkinan dan dampaknya, prioritas risiko, dan pemetaan risiko terhadap kontrol TI. Dokumentasi penilaian risiko berfungsi sebagai dasar untuk rencana audit dan memberikan masukan yang berharga untuk keseluruhan proses manajemen risiko organisasi.

Penilaian Risiko Audit TI adalah fase kritis yang membantu auditor mengidentifikasi, menilai, dan memprioritaskan risiko potensial terhadap sistem, proses, dan kontrol TI organisasi. Dengan mempertimbangkan faktor-faktor seperti ukuran, kompleksitas, dan persyaratan peraturan organisasi, auditor dapat mengembangkan pendekatan audit yang terfokus dan berbasis risiko, memastikan bahwa upaya mereka diarahkan ke area perhatian yang paling signifikan.

3.3.3 Evaluasi Kontrol (*Control Evaluation*)

Evaluasi Kontrol membantu auditor menentukan kecukupan dan efektivitas pengendalian TI organisasi dalam mengurangi risiko yang teridentifikasi. Fase ini dapat dijabarkan sebagai berikut:

1. **Memahami kontrol TI:**
   Kontrol TI adalah kebijakan, prosedur, dan alat yang diterapkan oleh organisasi untuk melindungi aset TI, memastikan integritas dan ketersediaan data, dan menjaga kepatuhan terhadap persyaratan peraturan. Kontrol dapat diklasifikasikan ke dalam berbagai kategori, seperti kontrol preventif, detektif, atau korektif, dan dapat berupa manual atau otomatis.
2. **Menilai desain kontrol:**
   Evaluasi desain kontrol melibatkan pemeriksaan apakah kontrol dirancang dengan tepat untuk mengatasi risiko yang teridentifikasi. Auditor menilai apakah pengendalian selaras dengan tujuan organisasi, praktik terbaik industri, dan persyaratan peraturan. Ini melibatkan peninjauan kebijakan kontrol, prosedur, dan konfigurasi sistem untuk memastikan mereka dirancang untuk beroperasi secara efektif di lingkungan TI organisasi.

3. **Menilai efektivitas pengendalian:**
   Evaluasi efektivitas pengendalian melibatkan penentuan apakah pengendalian beroperasi sebagaimana dimaksud dan efektif dalam mengurangi risiko yang terkait. Auditor biasanya menggunakan kombinasi teknik untuk menilai efektivitas pengendalian, termasuk:
   - Meninjau dokumentasi: Auditor memeriksa kebijakan, prosedur, log sistem, dan dokumentasi lain untuk memverifikasi bahwa kontrol telah diterapkan dan diikuti.
   - Mewawancarai personel: Auditor terlibat dalam diskusi dengan personel yang relevan, seperti staf TI, manajemen, dan pengguna akhir, untuk mendapatkan wawasan tentang pemahaman mereka tentang kontrol, peran dan tanggung jawab mereka, dan masalah apa pun yang mungkin mereka temui.
   - Melakukan penelusuran: Auditor mengamati tindakan kontrol, menelusuri transaksi atau proses melalui lingkungan TI untuk memastikan bahwa kontrol berfungsi seperti yang dirancang.
   - Pengujian: Auditor melakukan pengujian terhadap pengendalian untuk memvalidasi keefektifannya. Ini mungkin melibatkan pemilihan sampel, menggunakan alat otomatis, atau menerapkan berbagai teknik pengujian seperti penyelidikan, observasi, inspeksi, kinerja ulang, dan analisis data.
4. **Mengidentifikasi kesenjangan kontrol dan kekurangan:**
   Selama fase evaluasi pengendalian, auditor dapat mengidentifikasi kesenjangan atau kekurangan pengendalian. Ini dapat mencakup kontrol yang hilang, tidak memadai, atau tidak efektif yang gagal mengatasi risiko terkait. Auditor mendokumentasikan masalah ini dan dapat memberikan rekomendasi perbaikan untuk

membantu organisasi memperkuat lingkungan kontrol TI-nya.

5. **Menilai keseluruhan lingkungan pengendalian:**
   Selain mengevaluasi kontrol TI individu, auditor menilai lingkungan kontrol organisasi secara keseluruhan. Ini melibatkan faktor pertimbangan seperti proses manajemen risiko organisasi, nada di atas, dan tingkat tata kelola TI yang ada. Lingkungan pengendalian yang kuat dapat meningkatkan efektivitas pengendalian individu dan mengurangi kemungkinan kegagalan pengendalian.
6. **Mendokumentasikan temuan evaluasi kontrol:**
   Hasil evaluasi pengendalian harus didokumentasikan dengan cara yang jelas dan konsisten. Dokumentasi ini harus mencakup deskripsi pengendalian yang dinilai, metode evaluasi yang digunakan, kesenjangan atau kekurangan pengendalian yang teridentifikasi, dan setiap rekomendasi untuk perbaikan. Temuan evaluasi pengendalian berfungsi sebagai dasar untuk laporan audit dan memberikan masukan yang berharga bagi manajemen organisasi untuk mengatasi masalah yang teridentifikasi.

Evaluasi Kontrol Audit TI adalah fase kritis yang membantu auditor menilai desain dan efektivitas kontrol TI organisasi dalam mengurangi risiko yang teridentifikasi. Dengan meninjau dokumentasi, mewawancarai personel, dan melakukan penelusuran dan pengujian, auditor dapat mengidentifikasi kesenjangan dan kekurangan kontrol, memberikan wawasan berharga dan rekomendasi perbaikan untuk memperkuat lingkungan kontrol TI organisasi.

3.3.4 Pengujian (*Testing*)

Pengujian Audit TI memberikan bukti untuk mendukung kesimpulan auditor tentang efektivitas kontrol TI organisasi. Fase ini dapat dijabarkan sebagai berikut:

1. **Perencanaan tes:**
   Sebelum melakukan pengujian, auditor mengembangkan rencana pengujian yang menguraikan tujuan pengujian, pengendalian spesifik yang akan diuji, metodologi pengujian, ukuran sampel, dan hasil yang diharapkan. Rencana pengujian harus diselaraskan dengan ruang lingkup audit, tujuan, dan temuan penilaian risiko.
2. **Teknik pengujian:**
   Auditor menggunakan berbagai teknik pengujian untuk memvalidasi efektivitas pengendalian TI. Beberapa teknik umum meliputi:
   - Permintaan: Auditor mengumpulkan informasi dari personel melalui wawancara atau kuesioner untuk memahami pengetahuan mereka tentang kontrol, peran, dan tanggung jawab.
   - Pengamatan: Auditor mengamati proses dan kontrol dalam tindakan untuk memverifikasi fungsi yang tepat dan kepatuhan terhadap kebijakan dan prosedur.
   - Inspeksi: Auditor meninjau dokumentasi, seperti kebijakan, prosedur, log sistem, dan laporan, untuk memverifikasi keberadaan dan penerapan pengendalian yang tepat.
   - Kinerja ulang: Auditor secara independen melaksanakan kontrol atau proses untuk mengonfirmasi keefektifannya dan memvalidasi keakuratan hasil organisasi.
   - Analisis data: Auditor menggunakan alat dan teknik analitik data untuk menganalisis volume data yang

besar, mengidentifikasi pola atau tren, dan mendeteksi anomali atau kegagalan kontrol.

3. **Sampling:**
   Sampling melibatkan pemilihan subset item atau transaksi untuk pengujian, yang memungkinkan auditor untuk menarik kesimpulan tentang seluruh populasi tanpa memeriksa setiap item. Auditor dapat menggunakan metode sampling statistik atau nonstatistik dan harus mempertimbangkan faktor-faktor seperti ukuran populasi, efektivitas pengendalian, dan tingkat keyakinan dan presisi yang diinginkan ketika menentukan ukuran sampel yang tepat. Pengambilan sampel dapat membantu auditor melakukan pengujian dengan lebih efisien dan hemat biaya sambil tetap memberikan bukti yang cukup untuk mendukung kesimpulan mereka.
4. **Alat otomatis:**
   Auditor dapat menggunakan alat otomatis untuk mendukung upaya pengujian mereka, terutama ketika berhadapan dengan volume data yang besar atau sistem yang kompleks. Alat ini dapat mencakup perangkat lunak analitik data, teknik audit berbantuan komputer (CAAT), atau perangkat lunak audit khusus. Alat otomatis dapat meningkatkan efisiensi dan keakuratan pengujian serta memberikan wawasan yang lebih mendalam tentang lingkungan TI organisasi.
5. **Mengevaluasi hasil tes:**
   Setelah melakukan pengujian, auditor menganalisis hasilnya untuk menentukan keefektifan pengendalian dan mengidentifikasi setiap kegagalan, kekurangan, atau kesenjangan pengendalian. Ini mungkin melibatkan membandingkan hasil tes dengan hasil yang diharapkan, menghitung tingkat kesalahan, atau mengidentifikasi pola ketidakpatuhan.

6. **Mendokumentasikan temuan pengujian:**
   Temuan pengujian harus didokumentasikan secara jelas, ringkas, dan konsisten, memberikan bukti yang cukup untuk mendukung kesimpulan auditor. Dokumentasi harus mencakup deskripsi pengujian yang dilakukan, ukuran sampel, teknik pengujian yang digunakan, hasil pengujian, dan setiap kegagalan atau kekurangan pengendalian yang teridentifikasi. Dokumentasi ini berfungsi sebagai dasar laporan audit dan memberikan masukan berharga bagi manajemen organisasi untuk mengatasi masalah yang teridentifikasi.

Pengujian Audit TI adalah fase kritis yang membantu auditor memvalidasi keefektifan kontrol TI organisasi dalam mengatasi risiko yang teridentifikasi. Dengan menerapkan berbagai teknik pengujian, seperti penyelidikan, observasi, inspeksi, kinerja ulang, dan analisis data, serta menggunakan alat sampling dan otomatis, auditor dapat mengumpulkan bukti yang cukup untuk mendukung kesimpulan mereka tentang lingkungan pengendalian TI. Hasil dan temuan pengujian berfungsi sebagai dasar untuk laporan audit dan memberikan wawasan yang berharga bagi manajemen organisasi untuk mengatasi setiap kegagalan, kekurangan, atau kesenjangan pengendalian yang teridentifikasi. Fase ini membantu memastikan bahwa kontrol TI berfungsi sebagaimana mestinya dan secara efektif mengurangi risiko TI organisasi.

3.3.5 Pelaporan (*Reporting*)

Pelaporan adalah fase akhir dari proses audit TI, di mana auditor mengkomunikasikan temuan dan rekomendasi mereka kepada manajemen organisasi dan pemangku kepentingan terkait lainnya. Fase ini dapat dijabarkan sebagai berikut:

1. **Ringkasan bisnis plan:**
   Ringkasan eksekutif memberikan ikhtisar tingkat tinggi tentang ruang lingkup, tujuan, dan temuan utama audit. Ini menyoroti masalah dan rekomendasi yang paling signifikan, memungkinkan pembaca untuk dengan cepat memahami kesimpulan utama dari audit.
2. **Uraian rinci tentang ruang lingkup dan tujuan:**
   Laporan harus mencakup deskripsi yang jelas dan ringkas tentang ruang lingkup dan tujuan audit, menjelaskan area spesifik lingkungan TI yang diperiksa dan tujuan audit. Ini membantu pemangku kepentingan memahami konteks dan batasan audit.
3. **Metodologi audit:**
   Laporan harus menjelaskan metodologi audit, termasuk proses penilaian risiko, pendekatan evaluasi pengendalian, dan teknik pengujian yang digunakan. Hal ini memberikan transparansi tentang bagaimana audit dilakukan dan dasar kesimpulan auditor.
4. **Risiko dan kontrol yang teridentifikasi:**
   Laporan tersebut harus memberikan penjelasan rinci tentang risiko yang teridentifikasi dan kontrol TI terkait yang dievaluasi selama audit. Ini mungkin termasuk ringkasan temuan penilaian risiko, penjelasan tentang desain dan efektivitas kontrol, dan setiap kesenjangan atau kekurangan kontrol yang teridentifikasi.
5. **Rekomendasi untuk perbaikan:**
   Laporan harus mencakup rekomendasi spesifik yang dapat ditindaklanjuti untuk mengatasi kelemahan atau kekurangan pengendalian yang teridentifikasi. Rekomendasi ini mungkin melibatkan penguatan pengendalian yang ada, penerapan pengendalian baru, atau peningkatan lingkungan pengendalian secara keseluruhan.

Setiap rekomendasi harus diprioritaskan berdasarkan risiko terkait dan dampak potensial terhadap organisasi.

6. **Kesimpulan:**
   Bagian kesimpulan laporan harus meringkas keseluruhan temuan dan memberikan pendapat tentang kecukupan dan efektivitas lingkungan pengendalian TI organisasi. Ini mungkin termasuk penilaian kepatuhan organisasi dengan persyaratan peraturan, keselarasan dengan praktik terbaik industri, atau kemampuan untuk mengelola risiko TI secara efektif.
7. **Distribusi dan komunikasi:**
   Laporan audit harus diserahkan kepada manajemen organisasi, komite audit, dan pemangku kepentingan terkait lainnya, seperti auditor eksternal atau regulator. Laporan tersebut dapat disajikan dalam pertemuan formal atau melalui saluran komunikasi lainnya, yang sesuai.
8. **Tanggapan dan tindak lanjut manajemen:**
   Setelah menerima laporan audit, manajemen organisasi harus meninjau temuan dan rekomendasi serta mengembangkan rencana untuk mengatasi setiap masalah yang teridentifikasi. Ini mungkin melibatkan penugasan tanggung jawab, pengaturan garis waktu, dan pengalokasian sumber daya untuk mengimplementasikan perubahan yang direkomendasikan. Auditor TI dapat dilibatkan dalam memantau kemajuan dan memberikan panduan atau bantuan, sesuai kebutuhan.

Singkatnya, Pelaporan Audit TI adalah fase kritis yang memungkinkan auditor untuk mengkomunikasikan temuan dan rekomendasi mereka kepada manajemen organisasi dan pemangku kepentingan lainnya. Laporan tersebut harus memberikan gambaran umum audit yang jelas, ringkas, dan komprehensif

3.3.6 Tindak Lanjut (*Follow-up*)

Tindak Lanjut adalah fase penting dari proses audit TI, memastikan bahwa organisasi mengambil tindakan yang tepat untuk mengatasi temuan dan rekomendasi dari laporan audit. Fase ini dapat dijabarkan sebagai berikut:

1. **Pemantauan implementasi rekomendasi:**
   Fase tindak lanjut dimulai dengan memantau kemajuan organisasi dalam mengimplementasikan perubahan yang direkomendasikan. Auditor dapat bekerja sama dengan manajemen organisasi untuk melacak status tindakan korektif, memberikan panduan, dan memastikan bahwa rekomendasi ditangani tepat waktu.
2. **Mengevaluasi efektivitas tindakan korektif:**
   Setelah organisasi menerapkan perubahan yang direkomendasikan, auditor mengevaluasi keefektifan tindakan korektif dalam mengatasi masalah yang teridentifikasi. Ini mungkin melibatkan penilaian ulang risiko terkait, evaluasi ulang kontrol yang relevan, atau melakukan pengujian tambahan untuk memastikan bahwa kekurangan atau kesenjangan kontrol telah diatasi.
3. **Melakukan pengujian tambahan, wawancara, dan ulasan:**
   Fase tindak lanjut mungkin melibatkan kombinasi pengujian, wawancara, dan tinjauan dokumentasi untuk mengumpulkan bukti yang cukup untuk mendukung kesimpulan auditor tentang keefektifan tindakan korektif. Ini mungkin termasuk:
   - Pengujian: Auditor melakukan pengujian pada kontrol yang diperbarui untuk memvalidasi keefektifannya dalam mengurangi risiko terkait.
   - Wawancara: Auditor terlibat dalam diskusi dengan personel yang relevan untuk memahami pengetahuan mereka tentang kontrol yang diperbarui, peran dan

tanggung jawab mereka, dan masalah apa pun yang mungkin mereka temui selama proses implementasi.
- Tinjauan dokumentasi: Auditor memeriksa kebijakan, prosedur, konfigurasi sistem yang diperbarui, atau dokumentasi relevan lainnya untuk memverifikasi bahwa perubahan yang direkomendasikan telah diterapkan dengan benar dan diikuti sebagaimana dimaksud.

4. **Pelaporan kegiatan tindak lanjut:**
   Setelah menyelesaikan kegiatan tindak lanjut, auditor dapat menyiapkan laporan tindak lanjut atau memutakhirkan laporan audit asli untuk mendokumentasikan temuan dan kesimpulan mereka terkait penerapan rekomendasi. Laporan ini harus mencakup ringkasan tindakan korektif yang diambil, hasil pengujian tambahan, wawancara, dan ulasan, serta masalah atau masalah lainnya yang perlu ditangani.
5. **Mengkomunikasikan hasil tindak lanjut:**
   Hasil tindak lanjut harus dikomunikasikan kepada manajemen organisasi, komite audit, dan pemangku kepentingan terkait lainnya. Ini mungkin melibatkan penyajian temuan dalam pertemuan formal atau melalui saluran komunikasi lain, yang sesuai. Hasil tindak lanjut memberikan umpan balik yang berharga tentang kemajuan organisasi dalam menangani temuan audit dan membantu memastikan peningkatan berkelanjutan dalam lingkungan pengendalian TI.
6. **Pemantauan berkelanjutan dan perbaikan berkelanjutan:**
   Fase tindak lanjut bukanlah kegiatan satu kali; itu harus menjadi proses berkelanjutan yang membantu organisasi mempertahankan dan meningkatkan lingkungan kontrol TI dari waktu ke waktu. Auditor dapat terus memantau

kemajuan organisasi dalam mengatasi masalah atau masalah yang tersisa dan memberikan panduan dan dukungan sesuai kebutuhan. Keterlibatan berkelanjutan ini membantu memastikan bahwa organisasi tetap responsif terhadap risiko yang berkembang, persyaratan peraturan, dan praktik terbaik industri.

Fase Tindak Lanjut Audit TI adalah komponen penting dari proses audit TI, karena memastikan bahwa organisasi mengambil tindakan yang tepat untuk menangani temuan dan rekomendasi audit. Dengan memantau penerapan tindakan korektif, mengevaluasi keefektifannya, dan melakukan pengujian tambahan, wawancara, dan tinjauan, auditor dapat memastikan bahwa masalah yang teridentifikasi telah ditangani dan membantu organisasi memelihara dan meningkatkan lingkungan pengendalian TI-nya.

3.4 Kesimpulan

Proses audit TI adalah pendekatan yang sistematis dan komprehensif untuk mengevaluasi lingkungan pengendalian TI organisasi, menilai kemampuannya untuk memitigasi risiko, dan memastikan kepatuhan terhadap persyaratan peraturan dan praktik terbaik industri. Proses audit TI memainkan peran penting dalam menjaga aset TI organisasi, menjaga kerahasiaan, integritas, dan ketersediaan informasi, serta mendukung pencapaian tujuan bisnis.

Proses audit TI dapat dipecah menjadi beberapa fase utama, termasuk Perencanaan, Penilaian Risiko, Evaluasi Kontrol, Pengujian, Pelaporan, dan Tindak Lanjut. Setiap fase berkontribusi untuk membangun pemahaman menyeluruh tentang lingkungan TI organisasi, mengidentifikasi potensi risiko dan kekurangan kontrol, serta memberikan rekomendasi yang dapat ditindaklanjuti untuk perbaikan.

Selama tahap Perencanaan, auditor menetapkan ruang lingkup dan tujuan audit, memilih kriteria audit, dan mengembangkan rencana audit yang menguraikan sumber daya, jadwal, serta peran dan tanggung jawab tim audit. Fase Penilaian Risiko melibatkan identifikasi dan memprioritaskan potensi risiko terhadap sistem, proses, dan kontrol TI organisasi, dengan mempertimbangkan faktor-faktor seperti ukuran, kompleksitas, dan persyaratan peraturan organisasi.

Fase Evaluasi Kontrol berfokus pada penilaian desain dan efektivitas kontrol TI organisasi, yang merupakan kebijakan, prosedur, dan alat yang digunakan untuk memitigasi risiko. Auditor meninjau dokumentasi, mewawancarai personel, dan melakukan penelusuran untuk mendapatkan pemahaman tentang kontrol yang ada. Pada fase Pengujian, auditor memvalidasi keefektifan kontrol dengan menggunakan berbagai teknik pengujian, seperti penyelidikan, observasi, inspeksi, kinerja ulang, dan analisis data, bersama dengan alat sampling dan otomatis.

Fase Pelaporan menggabungkan temuan audit ke dalam laporan formal yang mencakup ringkasan eksekutif, deskripsi terperinci tentang ruang lingkup, tujuan, metodologi, risiko dan kontrol yang teridentifikasi, dan rekomendasi untuk perbaikan. Manajemen rumah sakit meninjau laporan dan mengembangkan rencana untuk mengatasi masalah yang teridentifikasi. Terakhir, selama fase Tindak Lanjut, auditor memantau penerapan rekomendasi, mengevaluasi keefektifan tindakan korektif, dan melakukan pengujian tambahan, wawancara, atau tinjauan untuk mengonfirmasi bahwa masalah yang teridentifikasi telah ditangani.

Proses audit TI adalah komponen penting dari keseluruhan manajemen risiko dan kerangka tata kelola organisasi. Dengan melakukan audit TI secara teratur, organisasi dapat secara proaktif mengidentifikasi dan

mengatasi potensi risiko, kekurangan kontrol, dan area untuk perbaikan, sehingga meningkatkan keamanan dan keandalan lingkungan TI mereka secara keseluruhan. Proses audit TI juga membantu organisasi mempertahankan kepatuhan terhadap persyaratan peraturan yang terus berkembang dan tetap mengikuti praktik terbaik industri.

Dalam lanskap digital yang semakin kompleks dan saling terhubung saat ini, pentingnya proses audit TI yang kuat tidak dapat dilebih-lebihkan. Karena organisasi terus mengandalkan teknologi untuk mendukung operasinya, proses audit TI berfungsi sebagai alat vital untuk mengelola risiko, memastikan efektivitas kontrol TI, dan mendorong budaya peningkatan berkelanjutan. Dengan berinvestasi dalam proses audit TI yang komprehensif dan efektif, organisasi dapat melindungi aset TI mereka dengan lebih baik, meningkatkan lingkungan kontrol mereka, dan pada akhirnya, mencapai tujuan bisnis mereka.

DAFTAR PUSTAKA

Ackerman, M. *et al.* 2009. 'IT strategic audit plan', *Journal of Technology Research*, 1(1).

Hall, J. A. 2015. *Information Technology Auditing*. 4th edn. Cengage Learning.

Merhout, J. W. and Havelka, D. 2008. 'Information Technology Auditing: A Value-Added IT Governance Partnership between IT Management and Audit', *Communications of the Association for Information Systems*, 23(1). doi: 10.17705/1CAIS.02326.

Otero, A. R. 2018. *Information technology control and audit*. CRC Press.

Senft, S., Gallegos, F. and Davis, A. 2012. *Information Technology Control and Audit*. CRC Press.

Stoneburner, G., Goguen, A. and Feringa, A. 2002. *Risk management guide for information technology systems*.

BAB 4
AUDIT MENGGUNAKAN CAAT

Oleh Abdurrasyid

4.1 Pendahuluan

Jenis lain dari teknik perangkat lunak yang digunakan dalam audit TI adalah CAAT (*Computer Assisted Audit Tools/Techniques*). CAAT adalah sebuah program yang terkomputerisasi untuk menjalankan fungsi audit untuk menguji (baik secara langsung maupun tidak langsung) logika internal dari suatu aplikasi komputer yang digunakan untuk mengolah data sehingga akan mengotomatisasikan atau menyederhanakan proses audit**.**

American Institute of Certified Public Accountants mengeluarkan SAS No. 94, "of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit." SAS tidak mengubah persyaratan untuk melakukan pengujian substantif pada jumlah yang signifikan tetapi menyatakan, "Tidak praktis atau tidak mungkin untuk membatasi risiko deteksi ke tingkat yang dapat diterima dengan hanya melakukan pengujian substantif." Saat menilai keefektifan desain dan pengoperasian pengendalian TI, auditor (auditor TI atau keuangan) perlu mengevaluasi dan menguji pengendalian ini. Keputusan untuk mengevaluasi dan menguji tidak terkait dengan ukuran organisasi tetapi kompleksitas lingkungan TI.

CAAT dapat digunakan oleh auditor TI atau keuangan dalam berbagai cara untuk mengevaluasi integritas aplikasi, menentukan kepatuhan terhadap prosedur, dan terus memantau hasil pemrosesan. Auditor TI, misalnya, meninjau

aplikasi untuk mendapatkan pemahaman tentang kontrol yang ada untuk memastikan keakuratan dan kelengkapan informasi yang dihasilkan.

Ketika kontrol aplikasi yang memadai diidentifikasi, auditor TI melakukan pengujian untuk memverifikasi desain dan keefektifannya. Ketika kontrol tidak memadai, auditor TI melakukan pengujian ekstensif untuk memverifikasi integritas data. Untuk melakukan pengujian aplikasi dan data, auditor dapat menggunakan CAAT.

Teknik otomatis telah terbukti lebih baik daripada teknik manual ketika berhadapan dengan volume informasi yang besar. Auditor, dengan menggunakan teknik otomatis, dapat mengevaluasi volume data yang lebih besar dan dengan cepat melakukan analisis data untuk mengumpulkan pandangan yang lebih luas dari suatu proses.

CAAT umum seperti *Audit Command Language* (ACL) dan *Interactive Data Extraction and Analysis* (IDEA) dapat digunakan untuk memilih sampel, menganalisis karakteristik file data, mengidentifikasi tren dalam data, dan mengevaluasi integritas data. Teknik lain yang digunakan untuk menganalisis data termasuk, misalnya, Microsoft Access dan Microsoft Excel. Microsoft Access dapat digunakan untuk menganalisis data, membuat laporan, dan menanyakan file data. Microsoft Excel juga dapat menganalisis data, membuat sampel, membuat grafik, dan melakukan analisis regresi atau tren. SAP Audit Management (bagian dari SAP *Assurance and Compliance Software* yang dilengkapi dengan SAP GRC) juga merampingkan proses audit dengan menyediakan alternatif yang hemat biaya untuk *spreadsheet* dan alat manual.* SAP Audit Management memfasilitasi dokumentasi bukti, pengaturan kertas kerja, dan pembuatan laporan audit. Teknik ini juga memberikan kemampuan analitis untuk mengalihkan fokus audit dari

menjamin hal-hal dasar menjadi memberikan wawasan dan saran.

4.2 Fungsi Audit

Sebagian besar keterampilan profesional yang diperlukan untuk menggunakan CAAT terletak pada perencanaan, pemahaman, dan pengawasan (misalnya, SAS No. 108—Perencanaan dan Pengawasan, dll.) teknik audit ini, dan pelaksanaan fungsi dan pengujian audit yang sesuai. Komputer memiliki berbagai kemampuan. Sebagai ilustrasi, tiga kategori besar fungsi audit komputer dapat diidentifikasi berdasarkan hal berikut:

1. Item-item untuk kepentingan audit
2. Audit perhitungan
3. Analisis data

4.2.1 Item-item untuk kepentingan audit

Auditor dapat menggunakan komputer untuk memilih item yang diminati, seperti item-item yang tidak biasa, atau sampel statistik dari item, misalnya dengan menetapkan kriteria spesifik untuk pemilihan item sampel, atau dengan menyatakan kriteria relatif dan membiarkan komputer melakukan pemilihan.

Contoh pemilihan berdasarkan kriteria tertentu mungkin berupa spesifikasi bahwa komputer mengidentifikasi semua transaksi senilai Rp 1.000.000 atau lebih dan menyiapkan laporan termasuk transaksi tersebut untuk tinjauan audit. Namun, auditor dapat mengambil pendekatan relatif dan menginstruksikan komputer untuk memilih transaksi terbesar yang merupakan 20% dari total nilai untuk kebutuhan tertentu.

Pendekatan ini meringkas prosedur audit manual karena auditor dapat mengandalkan pemilihan item yang

menjadi perhatian komputer. Jika komputer tidak digunakan, auditor harus memvalidasi proses seleksi. Dalam pendekatan tradisional, misalnya, auditor biasanya meminta personel organisasi atau klien untuk mendaftar semua transaksi senilai Rp1.000.000 atau lebih. Dengan komputer, auditor dapat diyakinkan bahwa CAAT yang digunakan telah melihat keseluruhan item hutang dagang, misalnya. Validasi proses seleksi melekat pada auditor dalam mengembangkan dan menerima program aplikasi audit komputer.

4.2.2 Audit perhitungan

Penerapan komputer dalam audit mampu menghemat waktu terutama jika perhitungan dapat dilakukan sebagai produk sampingan dari fungsi audit lainnya. Misalnya, komputer digunakan untuk memilih item penting dari file piutang. Dalam proses melihat file ini, komputer dapat diprogram untuk melihat dan mencatat semua transaksi penagihan. Karena kecepatan komputer, perhitungan ini dapat dilakukan pada seluruh item dalam file tanpa penambahan waktu atau biaya yang signifikan untuk pemrosesan ini.

Sedangkan pemeriksaan manual konvensional dapat menghabiskan waktu dan tenaga, biasanya, auditor harus membatasi pemeriksaan atas setiap penerapan yang diberikan pada perluasan dan sampel pertimbangan yang mencakup beberapa interval singkat dari periode yang diperiksa. Jelas, waktu yang dibutuhkan bisa jauh lebih tinggi ketika perhitungan verifikasi ini dilakukan pada file lengkap.

Ingat, bagaimanapun, bahwa komputer memiliki keterbatasan di area ini. Meskipun dapat diprogram untuk membuat banyak perbandingan dan pengujian logis, komputer tidak dapat menggantikan penilaian manusia dalam memeriksa item yang akan diuji.

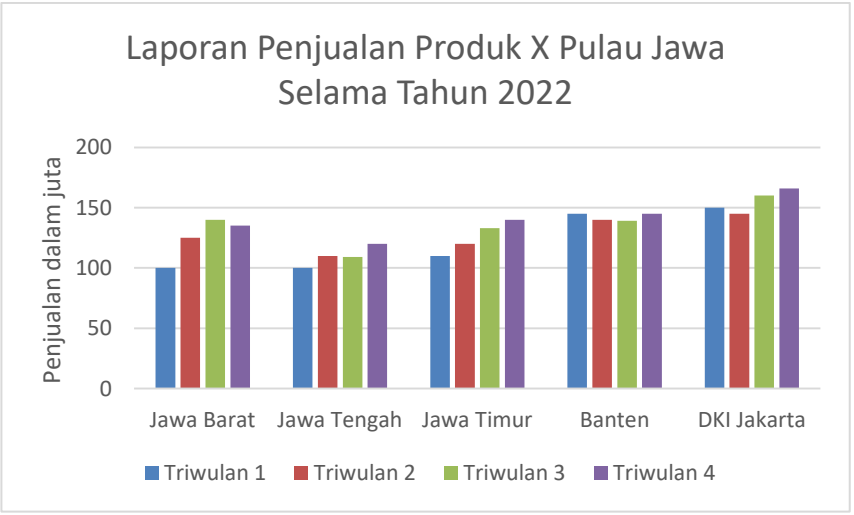
4.2.3 Analisis Data

Menggunakan komputer untuk analisis data merupakan peluang besar untuk inovasi oleh auditor. Komputer dapat membandingkan dan meringkas data dan dapat merepresentasikannya dalam bentuk grafik. Teknik yang dapat digunakan seperti:

1. Histogram
2. Pemodelan
3. Analisis Komparatif

Histogram adalah bagan batang yang menunjukkan hubungan grafik di antara strata data. Dalam audit berbantuan komputer, histogram biasanya menunjukkan distribusi frekuensi grafis dari rekaman di dalam file. Dengan menggambarkan hubungan ini dalam bentuk grafik seperti pada gambar 4.1, histogram memberikan perspektif yang lebih baik kepada auditor dalam analisis laporan keuangan. Histogram, pada dasarnya, adalah snapshot yang menunjukkan substansi, susunan, dan distribusi data dalam sistem akuntansi atau keuangan organisasi.

Auditor dapat menerapkan penilaian mereka dalam mengidentifikasi dan memilih teknik pengujian yang tepat dengan menggunakan histogram. Sebagai perbandingan, mengingat kumpulan data yang besar yang data distribusinya tidak diketahui, auditor melakukan pengujian secara relatif buta. Dalam kasus tersebut, auditor tidak dapat memastikan signifikansi data sampai setelah pengujian berjalan dengan baik. Dengan histogram, item penting untuk pengujian dapat diidentifikasi terlebih dahulu karena hubungannya dengan dunia akuntansi ditekankan secara grafis.



Gambar 4.1. Contoh histogram penjualan barang dalam 1 tahun

Pemodelan adalah teknik dimana auditor dapat membandingkan data saat ini dengan tren atau pola sebagai dasar untuk mengevaluasi kewajaran. Lihat Tampilan 4.2 untuk ilustrasi model perbandingan. Contoh pemodelan umum yang dikembangkan oleh auditor didasarkan pada laporan keuangan beberapa tahun. Komputer dapat menghasilkan laporan keuangan pro forma berdasarkan pendapatan masa lalu atau hubungan biaya. Pernyataan pro forma dibandingkan dengan laporan keuangan aktual sebagai uji kewajaran.

Gambar 4.2. Contoh perbandingan penjualan barang dalam 2 tahun terakhir

Pada **analisis komparatif**, teknik umum lainnya yang dapat digunakan dalam menganalisis data, adalah pemeriksaan audit hal ini terbukti efektif karna melibatkan perbandingan kumpulan data untuk menentukan hubungan yang mungkin menjadi kepentingan audit. Lihat Tampilan 4.1 untuk ilustrasi analisis laporan laba rugi komparatif.

Contoh analisis data umum lainnya menggunakan komputer untuk membandingkan file inventaris tahun-tahun sebelumnya dan saat ini. Variasi yang luas dalam saldo akhir tahun dapat menyebabkan tinjauan untuk kemungkinan keusangan. Kegagalan untuk mencocokkan nomor bagian dari tahun-tahun sebelumnya dan saat ini dapat memicu prosedur pengujian untuk menentukan apakah item lama telah dihapus atau yang baru ditambahkan.

Tabel 4.1. Contoh Analisis Laporan Laba Rugi Komparatif

Company XYZ				
Comparative Income Statement				
For the Years Ended December 31, 20X1 and 20X2 (in thousands except percent)				
	20X1	20X2	Increase(Decrease)	
	Amount	Amount	Amount	Percent
Sales	$840.0	$600	$240.0	40.0
Cost of Goods Sold	724.5	525	199.5	38.0
Gross Profit	$115.5	$75	$40.5	54.0
Selling Expenses	52.5	37.5	15.0	40.0
Administrative Expenses	41.4	30	11.4	38.0
Total Operating Expenses	$93.9	$67.5	$26.4	39.1
Income Before Income Tax	21.6	7.5	14.1	188.0
Income Tax Expense	10.8	2.7	8.1	300.0
Net Income	$10.8	$4.8	$6.0	125.0

Sumber:(Otero, 2020)

Analisis data, penting untuk melakukan fungsi dan pengujian audit, harus mengikuti pemahaman yang menyeluruh dan lengkap tentang sistem TI klien (yaitu, sistem informasi akuntansi). SAS No. 109, "Memahami Entitas dan Lingkungannya…," memperkuat pernyataan di atas, dan mengharuskan auditor untuk memahami lingkungan klien, yang mencakup sistem TI akuntansi dan keuangan mereka. Auditor biasanya menggunakan CAAT saat memahami dan memeriksa jenis sistem TI ini.

4.3 CAAT untuk Pengambilan Sampel

Beberapa teknik audit membantu dalam menentukan ukuran sampel dan memilih sampel. Misalnya, ACL secara otomatis menghitung ukuran sampel dan memilih sampel dari suatu populasi. Aplikasi spreadsheet juga menghasilkan angka acak untuk memilih sampel. Ada dua jenis teknik pengambilan sampel:

1. Sampling penilaian: Sampel yang dipilih didasarkan pada pengetahuan dan pengalaman auditor. Penilaiannya mungkin untuk memilih blok waktu, wilayah geografis, atau fungsi tertentu.
2. Sampling statistik: Sampel dipilih secara acak dan dievaluasi melalui penerapan teori probabilitas.

Kedua metode memungkinkan auditor memproyeksikan pada populasi. Namun, hanya pengambilan sampel statistik yang memungkinkan auditor untuk menghitung risiko bahwa sampel tersebut tidak mewakili populasi. Metode spesifik yang dipilih untuk sampel akan bergantung pada tujuan audit dan karakteristik populasi. Kesesuaian metode yang dipilih harus ditinjau untuk tujuan validitas oleh staf statistik atau aktuaria yang memiliki keahlian di bidang ini. Juga, metode pengambilan sampel yang diterapkan harus ditinjau kembali dan dinilai kembali dari waktu ke waktu untuk melihat apakah ada perubahan pada karakteristik atau atribut populasi yang ditinjau. Dua metode sampling statistik umum adalah:
Sampling Atribut Acak dan Sampling Variabel.

4.3.1 Sampling Atribut Acak dan Sampling Variabel

Pengambilan sampel atribut acak adalah teknik statistik yang menguji atribut transaksi tertentu yang telah ditentukan sebelumnya yang dipilih secara acak dari sebuah file. Atribut pengujian tersebut dapat mencakup tanda tangan, distribusi akun, dokumentasi, dan kepatuhan terhadap kebijakan dan

prosedur. Untuk melakukan sampling atribut, auditor harus menentukan tiga parameter yang menentukan ukuran sampel:

1. Perkirakan "tingkat kesalahan yang diharapkan", atau perkiraan persentase pengecualian transaksi, dalam total populasi.
2. Tentukan "ketepatan" yang diperlukan, atau tingkat akurasi yang diinginkan, dari kesimpulan sampel yang akan dibuat.
3. Tetapkan "tingkat kepercayaan" yang dapat diterima bahwa kesimpulan yang diambil dari sampel akan mewakili populasi.

Ukuran sampel akan ditentukan oleh kombinasi parameter tingkat kesalahan yang diharapkan, presisi, dan tingkat kepercayaan.

Pengambilan sampel variabel adalah teknik statistik lain yang memperkirakan nilai mata uang tertentu suatu populasi atau beberapa karakteristik terukur lainnya. Untuk menentukan ukuran sampel menggunakan sampling variabel, auditor harus menentukan empat parameter:

1. "Tingkat kepercayaan" yang dapat diterima bahwa kesimpulan yang ditarik dari sampel akan mewakili populasi.
2. Nilai absolut dari "populasi" untuk bidang yang dijadikan sampel.
3. "Materialitas" atau jumlah kesalahan maksimum yang diperbolehkan dalam populasi tanpa terdeteksi.
4. "*Expected error rate*" atau perkiraan persentase pengecualian transaksi dalam total populasi.

Ukuran sampel akan ditentukan oleh kombinasi keempat parameter yang tercantum di atas.

Tabel 4.2 menjelaskan teknik pengambilan sampel statistik lainnya yang biasa digunakan. Sekali lagi, auditor harus memperhatikan perubahan dan pembaruan panduan dalam penggunaan sampling untuk melakukan pekerjaan audit.

Contoh yang baik adalah SAS No. 111 (Amandemen Pernyataan Standar Audit No. 39, Audit Sampling). SAS No. 111 membahas konsep penetapan "tingkat penyimpangan yang dapat ditoleransi" saat pengambilan sampel uji pengendalian seperti pencocokan dan otorisasi. Ini juga mendefinisikan penggunaan yang tepat dari pengambilan sampel tujuan ganda(dual-purpose sampling).

Tabel 4.2. Teknik sampling yang biasa digunakan

Teknik Sampling	**Deskripsi**
Random Number Sampling	Item dipilih secara acak dari populasi sehingga setiap item memiliki peluang yang sama untuk dipilih.
Systematic Sampling (Interval Sampling)	Metode pengambilan sampel acak yang memulai sampel dengan memilih titik awal acak dalam populasi dan kemudian memilih item yang tersisa pada interval tetap. Metode ini tidak boleh digunakan untuk seleksi dari populasi yang memiliki pola tetap.
Stratified Sampling	Metode pengambilan sampel acak yang memisahkan populasi menjadi kelompok homogen sebelum memilih sampel acak. Metode ini harus digunakan untuk seleksi dari populasi dengan varians nilai yang luas.

Teknik Sampling	Deskripsi
Cluster Sampling (Block Sampling)	Metode pengambilan sampel acak yang memisahkan populasi ke dalam kelompok yang sama, dan kemudian memilih sampel acak dari kelompok tersebut.
Stop-or-go Sampling (Sequential Sampling)	Meminimalkan ukuran sampel dengan mengasumsikan tingkat kesalahan yang rendah. Ini memperkirakan tingkat kesalahan populasi dalam interval tertentu (misalnya, angka plus atau minus, dll.).
Discovery Sampling	Tes untuk kesalahan atau ketidakteraturan yang signifikan. Seharusnya tidak digunakan di mana ada kondisi menyimpang yang diketahui.
Dollar-unit Sampling (Probability Proportional to Size)	Metode ini menggunakan dolar sebagai unit pengambilan sampel, yang meningkatkan probabilitas bahwa nilai dolar yang lebih besar akan dipilih Ini terutama mendeteksi kelebihan pembayaran.
Mean Per Unit	Nilai rata-rata sampel dihitung dan dikalikan dengan unit dalam populasi untuk memperkirakan nilai total populasi.
Difference Estimation	Perbedaan rata-rata antara nilai audit dan nilai buku untuk unit sampel dihitung Perbedaan ini kemudian dikalikan dengan populasi untuk memperkirakan nilai total.

Teknik Sampling	Deskripsi
Ratio Estimation	Rasio sampel terhadap nilai buku dikalikan dengan nilai buku populasi untuk memperkirakan nilai total.

4.4 CAAT untuk Tinjauan Aplikasi

Ada berbagai CAAT yang berguna saat mengaudit aplikasi dan integritas data. Contoh dari teknik tersebut termasuk perangkat lunak audit umum. Perangkat lunak audit umum dapat digunakan antara lain untuk menganalisis logika spreadsheet dan perhitungan untuk akurasi dan kelengkapan, mengevaluasi data yang dihasilkan dari aplikasi (berada di database), dan menghasilkan bagan alur data logis. Dalam mengaudit database, misalnya, teknik yang berkaitan dengan penambangan data dapat mencari "melalui sejumlah besar data terkomputerisasi untuk menemukan pola atau tren yang berguna."* Teknik penambangan data membantu menganalisis data dari perspektif yang berbeda dan meringkasnya menjadi informasi yang berguna.

Contoh terkait lainnya termasuk analitik data (DA), atau prosedur untuk memeriksa data mentah untuk menarik kesimpulan. DA digunakan di banyak industri untuk memungkinkan pengambilan keputusan yang lebih baik, dan dalam sains untuk memverifikasi atau menyangkal model atau teori yang ada. DA membedakan dari data mining berdasarkan ruang lingkup, tujuan, dan fokus analisis. Penambangan data menyortir data dalam jumlah besar menggunakan perangkat lunak canggih untuk mengidentifikasi pola yang belum ditemukan dan membangun hubungan tersembunyi. DA, di sisi lain, berfokus pada proses menarik kesimpulan (atau menyimpulkan) hanya berdasarkan apa yang sudah diketahui.

Perangkat lunak audit umum memungkinkan untuk melakukan fungsi yang diperlukan secara langsung pada file aplikasi karena menggunakan spesifikasi yang disediakan auditor untuk menghasilkan program yang menjalankan fungsi audit. Auditor keuangan, misalnya, menggunakan perangkat lunak audit umum untuk:

1. Analisis dan bandingkan file
2. Pilih catatan khusus untuk pemeriksaan
3. Melakukan sampel acak
4. Validasi perhitungan
5. Siapkan surat konfirmasi
6. Menganalisis umur file transaksi

Perangkat lunak audit umum memungkinkan auditor TI untuk mengevaluasi kontrol aplikasi serta melakukan query dan menganalisis data terkomputerisasi untuk pengujian audit substantif. Beberapa perangkat lunak paling populer termasuk Audit Analytics oleh Arbutus Software, TopCAATs, CaseWare Analytics IDEA Data Analysis, Easy2Analyse, TeamMate, dan ACL. Ini semua hampir serupa dalam hal fungsionalitas.

4.4.1 *Audit Command Language* (ACL)

ACL adalah perangkat lunak audit umum yang membaca dari sebagian besar format (mis., database, file terbatas, file teks, file Excel, dll.) dan menyediakan pemilihan, analisis, dan pelaporan data. Lebih khusus lagi, ACL adalah alat interogasi file yang dirancang untuk membantu audit aplikasi karena dapat menangani dan memproses data dalam jumlah besar. Fungsi ACL berkisar dari: (1) mengidentifikasi saldo negatif, minimum, dan maksimum; (2) melakukan sampling statistik dan analisis penuaan; (3) mengidentifikasi duplikat atau celah dalam pengujian berurutan; dan (4) melakukan penggabungan dan pencocokan komparatif; diantara yang lain.

Manfaat dalam ACL meliputi:

1. Memberikan gambaran umum yang efektif pada format dan struktur file
2. Kemampuan untuk mengimpor berbagai jenis file data mentah
3. Pembuatan sampel dan ringkasan audit dengan mudah
4. Peningkatan cakupan pengujian dan peningkatan efisiensi
5. Skrip yang dapat dieksekusi pada periode saat ini dan selanjutnya
6. Kotak dialog untuk digunakan dalam aplikasi interaktif
7. Peningkatan pemahaman proses dan sistem dari lingkungan yang kompleks
8. Mengurangi prosedur manual

Beberapa fitur ACL umum meliputi:

- Menentukan dan mengimpor data ke ACL. Menentukan jenis data organisasi atau klien yang akan digunakan untuk tujuan analisis ACL adalah salah satu langkah terpenting saat menggunakan ACL. Auditor perlu mengidentifikasi dua hal: **pertama**, lokasi data yang akan digunakan; **kedua**, format dan struktur data tersebut.

  Untuk menghindari masalah saat mengakses data atau mengakses hard disk yang dilindungi secara tidak sengaja, dll., sebaiknya auditor meminta personel organisasi atau klien untuk menempatkan data yang diperlukan untuk analisis ke dalam hard disk terpisah (misalnya, hard disk USB auditor). , CD, hard drive terpisah, dll.).

  ACL memiliki kemampuan untuk membaca dan mengimpor data dari file carriage return (CR) (laporan teks biasa di mana CR menandai akhir setiap catatan); database, seperti dBASE, DB2, dan Open Database Connectivity (ODBC) (mis., MS Access, MS Excel, Oracle, dll.); file datar (data disusun berurutan dalam baris); dan file yang dibatasi (kolom dipisahkan dengan koma, titik koma, dll.). Jenis file lain

yang dibaca oleh ACL termasuk file laporan, file tersegmentasi, file dengan panjang variabel, file CR/Line Feed (LF), sumber data dengan atau tanpa tata letak file, file dengan panjang tetap, file LF, database mainframe, dan multiple- file tipe record.

- Menyesuaikan tampilan. Dengan ACL, auditor dapat mengubah tampilan file asli yang didefinisikan menjadi tampilan yang lebih sesuai dengan analisis data yang dimaksud. ACL juga memungkinkan auditor untuk membuat tampilan baru atau mengubah tampilan yang sudah ada tanpa "menyentuh" data sebenarnya dari file. Ini berarti bahwa perubahan untuk melihat data hanya untuk tujuan presentasi dan oleh karena itu tidak akan mengubah atau menghapus data.
- Menyaring data. Filter mudah dibuat di ACL dan berguna untuk analisis cepat dan total kontrol setelah file diimpor. Memfilter data melalui ACL memungkinkan auditor untuk mendukung pengujian dan analisis mereka. Pemfilteran di ACL menggunakan operator logis (mis., DAN, ATAU, BUKAN, dll.) sebagai kondisi untuk secara efektif menghasilkan informasi yang sesuai dengan kriteria tertentu. Misalnya, auditor dapat mencari entri jurnal akuntansi tertentu yang diposting di hari libur atau di luar jam kerja. ACL akan memungkinkan informasi berbasis kondisi tersebut diproduksi untuk analisis. Ada dua jenis filter:

  filter global dan **filter perintah**. Filter global, saat diaktifkan, berlaku untuk semua perintah dan semua tampilan untuk tabel aktif. Filter global tetap di tempatnya hingga dihapus atau hingga tabel ditutup.

  Filter perintah, di sisi lain, berlaku untuk satu perintah dan tetap berlaku hanya sampai ACL memproses perintah

tersebut. Filter dapat diberi nama, disimpan, dan digunakan kembali bila diperlukan.

- Analisis data. Auditor menggunakan ACL untuk mengevaluasi dan mengubah data menjadi informasi yang dapat digunakan. Data dapat dalam berbagai ukuran, format, dan dari hampir semua platform. Baik penalaran analitis dan logis digunakan untuk memeriksa setiap komponen data, dan menyaring makna bahkan dari sejumlah besar data. Perintah ACL di tabel 4.3 biasanya digunakan untuk melakukan tugas analisis data.

Tabel 4.3. Perintah ACL yang biasa digunakan dalam analisis data

ACL Command	Description
Extract	Memilih rekaman atau bidang dari file atau tabel saat ini, dan menyalinnya ke file atau tabel lain.
Export	Mengirim data ke file eksternal (misalnya, database, Excel, file teks, dll.) untuk digunakan di luar ACL.
Sorting	Mengurutkan atau mengatur tabel aktif ke dalam urutan naik atau turun berdasarkan bidang kunci yang ditentukan.
Verify	Memeriksa kesalahan validitas data dalam tabel aktif. Memastikan bahwa data dalam tabel sesuai dengan tata letak tabel dan melaporkan kesalahan yang terjadi.
Search	Menempatkan rekaman pertama dalam tabel terindeks yang memenuhi kriteria/kondisi tertentu.
Append	Menambahkan output perintah ke akhir file yang ada alih-alih menimpa file yang ada.

ACL Command	Description
Count	Menjumlahkan jumlah rekaman dalam tabel saat ini, atau hanya rekaman yang memenuhi kriteria atau kondisi pengujian tertentu.
Total	Menjumlahkan bidang numerik atau ekspresi dalam tabel aktif.
Statistical	Digunakan pada bidang tanggal dan numerik untuk mendapatkan gambaran umum data. Perintah Statistik menghasilkan (1) jumlah rekaman, total bidang, dan nilai bidang rata-rata untuk nilai bidang positif, nol, dan negatif; (2) nilai absolut; (3) rentang; dan (4) nilai bidang tertinggi dan terendah.
Stratify	Memungkinkan tampilan distribusi catatan yang jatuh ke dalam interval atau strata yang ditentukan. Artinya, ini menghitung jumlah rekaman yang jatuh ke dalam interval tertentu dari bidang numerik atau nilai ekspresi, dan subtotal satu atau lebih bidang untuk setiap strata.
Classify	Menghitung jumlah catatan yang berkaitan dengan setiap nilai unik bidang karakter dan subtotal bidang numerik yang ditentukan untuk masing-masing nilai unik ini.
Histogram	Memberikan gambaran umum tentang konten tabel. Secara khusus, ini menghasilkan grafik batang vertikal 3-D dari distribusi rekaman di atas nilai bidang atau ekspresi.
Age	Menghasilkan ringkasan data yang sudah

ACL Command	Description
	tua (misalnya, klasifikasi faktur yang belum dibayar)
Summarize	Menghasilkan jumlah catatan dan total nilai bidang numerik untuk setiap nilai berbeda dari bidang karakter kunci dalam tabel yang diurutkan.
Examine Sequence	Menentukan apakah bidang kunci dalam tabel aktif berada dalam urutan berurutan, dan mendeteksi celah, duplikat, atau angka yang hilang dalam urutan.
Look for Gaps	Mendeteksi celah di bidang utama tabel saat ini (misalnya, kesenjangan dalam angka, tanggal, dll.)
Look for Duplicates	Mendeteksi apakah field kunci dalam tabel saat ini berisi duplikat dalam urutan.
Sampling	ACL menawarkan banyak metode pengambilan sampel untuk analisis statistik. Dua yang paling sering digunakan adalah record sampling (RS) dan monetary unit sampling (MUS), keduanya dibuat dari populasi dalam tabel. Setiap metode memungkinkan pengambilan sampel acak dan interval. MUS mengekstrak rekaman sampel dari kumpulan data. MUS biasanya digunakan jika file sangat miring dengan nilai besar Item. RS, di sisi lain, memperlakukan setiap catatan secara setara, menggunakan nilai nominal satu. RS digunakan ketika catatan dalam file didistribusikan secara merata di seluruh

ACL Command	Description
	data, sehingga setiap catatan memiliki peluang yang sama untuk dipilih. Pilihan metode akan tergantung pada tujuan keseluruhan pengambilan sampel serta komposisi file yang sedang diaudit.

Saat merencanakan proyek analisis data ACL, penting bagi auditor TI untuk mengikuti langkah-langkah di bawah ini:

1. Langkah 1: Mendapatkan data
2. Langkah 2: Mengakses data
3. Langkah 3: Memverifikasi integritas data
4. Langkah 4: Menganalisis dan menguji data
5. Langkah 5: Melaporkan temuan

Langkah 1: Mendapatkan Data

Auditor harus mengetahui data yang dia butuhkan untuk memenuhi tujuan proyek yang ditentukan. Untuk itu, auditor harus mengumpulkan informasi yang diperlukan dengan bertemu dengan berbagai organisasi dan/atau personel klien, termasuk, namun tidak terbatas pada, personel TI, MIS, dan/atau akuntansi atau keuangan untuk memahami data, ukurannya, formatnya, strukturnya. , dan bidang data yang diperlukan.

Langkah 2: Mengakses Data

Auditor harus terbiasa dengan data yang akan dikerjakannya, khususnya, file tempat data disimpan, struktur file, format, tata letak, ukuran, bidang data, jumlah catatan, dll. Auditor harus menilai data yang termasuk dalam file untuk

menentukan yang mana tugas analisis data harus digunakan dan platform atau lingkungan apa.

Langkah 3: Memverifikasi Integritas Data

Auditor harus memastikan bahwa data adalah data yang baik. Dengan kata lain, data yang akan dianalisis harus valid, akurat, dan lengkap, terutama saat bekerja dengan file data yang tidak diatur dalam catatan. ACL menyediakan alat seperti hitung, total, dan verifikasi untuk menangani jenis file data ini.

Langkah 4: Menganalisis dan Menguji Data

Data yang akan dianalisis dan diuji dapat dalam berbagai ukuran, format, dan dari hampir semua platform. Auditor menggunakan ACL untuk mengevaluasi dan mengubah data tersebut menjadi informasi yang bermakna yang dapat membantu proses pengambilan keputusan mereka. Ada beberapa perintah ACL yang biasanya digunakan saat melakukan jenis analisis dan pengujian data ini (lihat tabel 4.2).

Langkah 5: Melaporkan Temuan

Setelah menyelesaikan analisis dan pengujian data, auditor TI harus mempresentasikan dan mengkomunikasikan hasil dan temuan mereka dalam format yang mudah dibaca. Sebagai bagian dari pelaporan hasil, auditor harus memelihara tata letak file dan proyek ACL untuk tujuan cadangan dan memungkinkan rekreasi, jika perlu. Auditor harus menyertakan informasi terkait ACL dalam kertas kerja audit, termasuk, namun tidak terbatas pada, salinan program ACL, tata letak log/file ACL, dan permintaan data untuk audit tahun mendatang.

4.5 CAAT untuk Audit Pengendalian Aplikasi

Saat mengaudit pengendalian aplikasi, auditor memeriksa pengendalian input, pemrosesan, dan output yang spesifik untuk aplikasi tersebut. Kontrol aplikasi juga disebut sebagai "kontrol otomatis". Kontrol input otomatis

memvalidasi data yang dimasukkan ke dalam sistem, dan meminimalkan kemungkinan kesalahan dan kelalaian.
Contoh kontrol input termasuk memeriksa: karakter dalam field; tanda positif/negatif yang sesuai; jumlah terhadap nilai tetap/terbatas; jumlah terhadap batas bawah dan atas; ukuran data; dan kelengkapan data, antara lain. Kontrol pemrosesan adalah kontrol yang mencegah, mendeteksi, dan/atau

memperbaiki kesalahan saat memproses. Contoh pengendalian pemrosesan meliputi pencocokan data sebelum tindakan dilakukan (mis., mencocokkan jumlah faktur dengan pesanan pembelian dan laporan penerimaan, dll.), menghitung ulang total batch, menyilangkan data untuk memverifikasi keakuratan perhitungan, dan memastikan bahwa hanya yang benar dan paling file yang diperbarui digunakan. Kontrol keluaran mendeteksi kesalahan setelah pemrosesan selesai.

Contoh pengendalian keluaran termasuk melakukan rekonsiliasi data laporan (misalnya, buku besar dengan buku besar pembantu, dll.), meninjau laporan untuk akurasi dan kelengkapan (misalnya, melakukan perbandingan bidang data kunci, memeriksa informasi yang hilang, dll.), dan melindungi transfer data untuk memastikan data ditransmisikan secara lengkap dan memadai (mis., enkripsi, dll.).

CAAT sangat berguna bagi auditor saat mengevaluasi pengendalian aplikasi yang terkait dengan pemrosesan transaksi. Seperti dijelaskan di atas, kontrol terkait pemrosesan transaksi berkaitan dengan keakuratan, kelengkapan, validitas, dan otorisasi data yang ditangkap, dimasukkan, diproses, disimpan, dikirim, dan dilaporkan. Auditor biasanya bekerja dengan spreadsheet dan/atau database yang disediakan oleh organisasi atau klien saat melakukan prosedur mereka. Aplikasi kontrol yang ditemukan pada spreadsheet dan/atau database yang biasanya diuji oleh auditor antara lain adalah memeriksa keakuratan matematis catatan, memvalidasi input

data, dan melakukan pemeriksaan urutan numerik. Auditor harus memastikan jenis kontrol ini diterapkan secara efektif untuk memastikan hasil yang akurat.

4.5.1 Pengendalian Spreadsheet

Spreadsheet mungkin tampak relatif mudah karena penggunaannya yang meluas. Namun, risiko yang disajikan signifikan jika hasil spreadsheet diandalkan untuk pengambilan keputusan.

Kurangnya keandalan, kurangnya kemampuan audit, dan kurangnya kemampuan untuk dimodifikasi adalah semua risiko yang terkait dengan desain spreadsheet yang buruk. Auditor menggunakan CAAT untuk menilai spreadsheet yang disiapkan klien atau organisasi untuk menganalisis data mereka dan pada akhirnya membentuk opini. Kontrol harus diterapkan untuk meminimalkan risiko data yang buruk dan logika yang salah, terutama jika spreadsheet digunakan kembali. Beberapa kontrol utama yang meminimalkan risiko dalam pengembangan dan penggunaan spreadsheet meliputi:

1. Analisis. Memahami persyaratan sebelum membuat spreadsheet
2. Sumber data. Jaminan bahwa data yang digunakan valid, andal, dan dapat diautentikasi ke sumber asal
3. Tinjauan desain. Tinjauan dilakukan oleh rekan atau profesional sistem
4. Dokumentasi. Rumus, perintah makro, dan setiap perubahan pada spreadsheet harus didokumentasikan secara eksternal dan di dalam spreadsheet
5. Verifikasi logika. Pemeriksaan dan perbandingan kewajaran dengan keluaran yang diketahui
6. Tingkat pelatihan. Pelatihan formal dalam desain spreadsheet, pengujian, dan implementasi
7. Jangkauan audit. Tinjauan desain informal atau prosedur audit formal

8. Mendukung komitmen. Pemeliharaan dan dukungan aplikasi yang berkelanjutan dari personel TI.

4.5.2 Pengendalian Database

Database departemen harus dilindungi dengan kontrol yang mencegah perubahan data yang tidak sah. Selain itu, setelah database diimplementasikan, database tersebut harus disimpan dalam direktori program terpisah dan dibatasi hanya untuk "eksekusi saja". Basis data juga dapat dilindungi dengan mengaktifkan kemampuan "hanya baca" kepada pengguna untuk data yang tetap statis. Hak akses harus diberikan kepada pengguna tertentu untuk tabel tertentu (grup akses). Layar input harus menyertakan kontrol pengeditan yang membatasi entri data ke opsi yang valid. Ini dapat dicapai dengan memiliki tabel nilai yang dapat diterima untuk field data. Keakuratan data juga dapat ditingkatkan dengan membatasi jumlah *free-form field* dan memberikan kode entri kunci dengan nilai pencarian untuk deskripsi lengkap. Kontrol yang umumnya diharapkan oleh auditor untuk diidentifikasi (dan pada akhirnya dinilai) dalam klien atau disiapkan oleh organisasi antara lain:

1. Integritas referensial. Cegah penghapusan nilai kunci dari tabel terkait
2. Integritas transaksi. Mengembalikan nilai transaksi yang gagal
3. Integritas entitas. Buat identifikasi catatan unik
4. Kendala nilai. Batasi nilai ke rentang yang dipilih
5. Perlindungan pembaruan bersamaan. Mencegah pertikaian data
6. Perlindungan pencadangan dan pemulihan. Kemampuan untuk mencadangkan informasi dan aplikasi penting dan memulihkan untuk melanjutkan

7. Menguji perlindungan. Lakukan pengujian di tingkat sistem, aplikasi, dan unit.

4.6 CAAT untuk Mereview Operasional

Sebelumnya, kami membahas sejumlah teknik yang digunakan untuk melakukan tugas guna mendukung audit aplikasi. Sebagian besar teknik ini dapat digunakan untuk mendukung tinjauan operasional serta mengumpulkan informasi tentang efektivitas pengendalian umum atas operasi TI. Namun, penggunaan teknik tidak perlu dibatasi pada paket khusus. Bahasa komputer dapat berguna dalam melakukan pengujian operasional dan mengumpulkan informasi tentang keefektifan pengendalian umum.

Bahkan alat dasar seperti Access di MS Office dapat digunakan untuk mengambil file data yang diimpor dari data operasional (misalnya informasi akun pengguna dan akses file, hak atas jumlah akses file, dll.), melakukan analisis pada file (histogram , frekuensi, ringkasan), lalu pindahkan data ke MS Excel dan gambarkan informasi secara visual untuk manajemen atau bahkan perkiraan tren sehubungan dengan beban kerja, pertumbuhan, dan area operasional TI lainnya.

Fokus tinjauan operasional adalah pada evaluasi efektivitas, efisiensi, dan pencapaian tujuan yang terkait dengan operasi manajemen sistem informasi. Langkah-langkah audit dasar dalam tinjauan operasional mirip dengan audit TI atau audit laporan keuangan, kecuali ruang lingkupnya. Spesifik kegiatan dalam tinjauan operasional meliputi:

1. Tinjau kebijakan dan dokumentasi pengoperasian
2. Konfirmasikan prosedur dengan manajemen dan personel pengoperasian
3. Amati fungsi dan aktivitas operasi
4. Memeriksa rencana dan laporan keuangan dan operasi
5. Uji keakuratan informasi pengoperasian

6. Uji kontrol operasional

4.7 Audit di Sekitar Komputer Versus Audit Melalui Komputer

Mungkin ada situasi di lingkungan TI di mana audit di sekitar komputer atau "pendekatan audit kotak hitam" mungkin lebih memadai daripada audit melalui komputer saat aplikasi otomatis relatif sederhana dan mudah. Saat melakukan audit di sekitar komputer, auditor memperoleh dokumen sumber yang terkait dengan transaksi masukan tertentu dan merekonsiliasi dokumen terhadap hasil output. Oleh karena itu, dokumentasi pendukung audit dibuat dan kesimpulan dicapai tanpa mempertimbangkan bagaimana masukan diproses untuk menghasilkan keluaran.

Sayangnya, SAS No. 94 tidak menghilangkan penggunaan teknik ini. Kelemahan utama audit di sekitar pendekatan komputer adalah tidak memverifikasi atau memvalidasi apakah logika program dari aplikasi yang diuji sudah benar. Ini adalah karakteristik audit melalui pendekatan komputer (atau “pendekatan audit kotak putih”).

Audit melalui pendekatan komputer mencakup berbagai teknik untuk mengevaluasi bagaimana aplikasi dan pengendalian yang tertanam di dalamnya merespons berbagai jenis transaksi (anomali) yang dapat mengandung kesalahan. Ketika audit melibatkan penggunaan teknologi canggih atau aplikasi yang kompleks, auditor TI harus menggunakan teknik yang dikombinasikan dengan alat untuk menguji dan mengevaluasi aplikasi dengan sukses. Pendekatan audit ini relevan mengingat peningkatan signifikan teknologi dan dampaknya terhadap proses audit. Teknik yang paling umum digunakan termasuk fasilitas pengujian terintegrasi, data pengujian, simulasi paralel, modul audit tertanam, file tinjauan audit kontrol sistem (scarf), dan penandaan transaksi. Sekali

lagi, banyak dari teknik ini harus disematkan ke dalam aplikasi untuk digunakan oleh auditor dan personel keamanan informasi. Teknik-teknik ini memberikan audit dan evaluasi terus-menerus terhadap aplikasi atau sistem dan memberikan jaminan kepada manajemen dan personel audit atau keamanan bahwa kontrol berfungsi seperti yang direncanakan, dirancang, dan diterapkan. Ini dijelaskan, dengan kelebihan dan kekurangannya, di Tabel 4.4 di bawah ini.

Tabel 4.4. Kelebihan Dan Kekurangan Teknik Audit

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
Integrated Test Facility	Fasilitas pengujian terintegrasi adalah lingkungan pengujian bawaan dalam suatu sistem. Pendekatan ini digunakan terutama dengan sistem online berskala besar yang melayani banyak lokasi di dalam perusahaan atau organisasi. Fasilitas pengujian terdiri dari perusahaan atau cabang fiktif, yang diatur dalam aplikasi dan struktur file untuk menerima atau memproses transaksi pengujian seolah-olah	Dirancang ke dalam aplikasi selama pengembangan sistem. (A) Keahlian diperlukan untuk merancang modul audit (lingkungan pengujian bawaan) ke dalam aplikasi dan untuk memastikan bahwa transaksi pengujian tidak memengaruhi data aktual. (D) Karena modul audit disiapkan di aplikasi organisasi atau klien, risiko gangguan data tinggi. Kontrol harus dirancang dan diimplementasikan secara memadai untuk

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
	itu adalah entitas operasi yang sebenarnya. Sepanjang periode keuangan, auditor dapat mengajukan transaksi untuk menguji sistem	mengidentifikasi dan menghilangkan pengaruh transaksi pengujian. (D)
Pengujian Data	Teknik ini melibatkan metode penyediaan transaksi uji ke sistem untuk diproses oleh aplikasi yang ada. Data uji menyediakan spektrum penuh transaksi untuk menguji proses dalam aplikasi dan sistem. Baik transaksi yang valid maupun yang tidak valid harus dimasukkan dalam data pengujian karena tujuannya adalah untuk menguji bagaimana sistem memproses input transaksi yang benar dan yang salah. Untuk layanan kartu	Keahlian minimal diperlukan untuk menjalankan teknik data uji. (A) Risiko mengganggu data organisasi atau klien minimal karena fakta bahwa salinan aplikasi digunakan. (A) Personil dari organisasi atau klien memberikan salinan aplikasi, namun mungkin sulit untuk menentukan apakah salinan yang diberikan tepat, sehingga mengurangi keandalan metode pengujian. (D)

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
	kredit konsumen, transaksi tersebut dapat berupa nomor rekening yang tidak valid, rekening yang telah ditangguhkan atau dihapus, dan lain-lain. Jika ketergantungan ditempatkan pada pengujian program, aplikasi, atau sistem, beberapa bentuk pengujian intermiten sangat penting. Generator data uji adalah alat yang sangat baik untuk mendukung teknik ini, tetapi tidak boleh diandalkan sepenuhnya untuk pengujian kondisi ekstrim	
Simulasi Paralel	Simulasi paralel melibatkan pemeliharaan terpisah dari dua set program yang mungkin identik. Kumpulan program	Risiko mengganggu organisasi atau data klien minimal. Simulasi tidak memengaruhi pemrosesan. (A) Auditor memperoleh informasi keluaran secara

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
	asli adalah salinan produksi yang digunakan dalam aplikasi yang sedang diperiksa. Set kedua dapat berupa salinan yang diamankan oleh auditor pada saat yang sama dengan versi aslinya dimasukkan ke dalam produksi. Saat perubahan atau modifikasi dilakukan pada program produksi, auditor membuat pembaruan yang sama pada salinannya. Jika tidak ada perubahan tanpa izin yang terjadi, dengan menggunakan input yang sama, membandingkan hasil dari setiap rangkaian program akan menghasilkan hasil yang sama. Cara lain bagi auditor untuk mengembangkan	langsung tanpa intervensi dari organisasi atau personel klien. (A) Sejauh mana keahlian diperlukan tergantung pada kompleksitas pemrosesan organisasi atau klien yang disimulasikan. (A atau D)

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
	pseudocode menggunakan bahasa tingkat tinggi (Vbasic, SQL, JAVA, dll.) dari dokumentasi dasar mengikuti logika proses dan persyaratan. Untuk tujuan audit, kedua aplikasi perangkat lunak (pengujian versus aktual) akan menggunakan input yang sama dan menghasilkan hasil independen yang dapat dibandingkan untuk memvalidasi langkah pemrosesan internal.	
Modul Audit Tertanam	Modul audit terprogram yang ditambahkan ke aplikasi yang sedang ditinjau.	Modul tertanam memungkinkan auditor untuk memantau dan mengumpulkan data untuk analisis dan untuk menilai risiko pengendalian dan efektivitas. (A) Tingkat keahlian yang dibutuhkan dianggap sedang hingga tinggi,

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
		karena auditor membutuhkan pengetahuan dan keterampilan dalam pemrograman untuk merancang dan mengimplementasikan modul. (D) Risiko mengganggu data klien mungkin tinggi. Karena semua transaksi akan tunduk pada algoritme penyaringan modul, ini dapat memengaruhi kecepatan pemrosesan secara signifikan. (D)
Systems Control Audit Review File (SCARF)	File Tinjauan Audit Kontrol Sistem (SCARF) adalah teknik waktu nyata lainnya yang dapat mengumpulkan transaksi atau proses tertentu yang melanggar kondisi atau pola tertentu yang telah ditentukan sebelumnya. Hal ini dapat ditingkatkan dengan perangkat	Izinkan auditor untuk menanamkan rutinitas audit ke dalam sistem aplikasi dan mengumpulkan data tentang peristiwa yang menarik bagi mereka. (A) Keahlian diperlukan untuk menanamkan rutinitas audit ke dalam sistem aplikasi, dan memastikan rutinitas tersebut tidak memengaruhi data aktual.

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
	lunak pendukung keputusan yang memperingatkan personel yang ditunjuk (audit, keamanan, dll.) tentang aktivitas yang tidak biasa atau hal-hal yang tidak biasa. Spesialis forensik komputer dapat mengumpulkan data ke file log untuk ditinjau dan diperiksa lebih lanjut	(D) Risiko mengganggu data organisasi atau klien tinggi. Kontrol harus dirancang dan diterapkan secara memadai untuk mengidentifikasi dan menghilangkan efek dari rutinitas audit tertanam. (D)
Tag Transaksi	Mengikuti transaksi yang dipilih melalui aplikasi mulai dari input, transmisi, pemrosesan, dan penyimpanan hingga outputnya untuk memverifikasi integritas, validitas, dan keandalan aplikasi. Beberapa aplikasi memiliki fungsi jejak atau debug, yang memungkinkan seseorang untuk	Tag transaksi dari awal sampai akhir. (A) Memungkinkan auditor untuk mencatat semua transaksi atau cuplikan aktivitas. (A) Keahlian diperlukan untuk menambahkan penunjukan khusus (atau tag) ke catatan transaksi. (D) Risiko mengganggu data klien mungkin sedang hingga tinggi. Kontrol harus dirancang dan diterapkan secara

Teknik Audit	Deskripsi	Kelebihan (A) dan Kekurangan (D)
	mengikuti transaksi melalui aplikasi. Ini mungkin cara untuk memastikan bahwa proses penanganan transaksi yang tidak biasa diikuti dalam modul dan kode aplikasi.	memadai untuk mengidentifikasi dan menghapus tag atau penunjukan khusus yang ditambahkan ke transaksi yang sedang dievaluasi. (D)

DAFTAR PUSTAKA

Otero, A. R. 2020. *Information Technology Control and Audit*. 5th edn. United States of America: CRC Press.

BAB 5
TEKNIK AUDIT PERANGKAT KERAS

Oleh Angga Aditya Permana

5.1 Pendahuluan

Kontrol dan audit teknologi informasi adalah dua konsep terkait yang digunakan untuk memastikan bahwa sistem dan proses teknologi informasi dalam suatu organisasi berjalan sesuai dengan tujuan dan kebijakan yang ditetapkan, serta memastikan bahwa informasi yang dihasilkan dan disimpan oleh sistem tersebut akurat, aman, dan dapat dipertanggungjawabkan.

Kontrol teknologi informasi merujuk pada proses untuk mengelola, memantau, dan melindungi sistem dan data teknologi informasi dalam suatu organisasi. Kontrol teknologi informasi meliputi semua kebijakan, prosedur, dan teknologi yang digunakan untuk memastikan bahwa sistem dan data tersebut terlindungi dari ancaman seperti hacking, virus, dan serangan siber lainnya. Kontrol teknologi informasi juga memastikan bahwa data yang disimpan oleh sistem tersebut akurat, relevan, dan dapat diandalkan.

Sementara itu, audit teknologi informasi adalah proses untuk mengevaluasi dan memverifikasi keamanan dan keandalan sistem dan data teknologi informasi dalam suatu organisasi. Audit teknologi informasi melibatkan pemeriksaan sistem, infrastruktur, dan aplikasi teknologi informasi yang digunakan dalam suatu organisasi. Tujuan dari audit teknologi informasi adalah untuk memastikan bahwa sistem dan data tersebut terlindungi dengan baik, bahwa kebijakan dan prosedur yang ditetapkan berfungsi dengan baik, dan bahwa

sistem dan data tersebut memenuhi persyaratan keamanan dan keandalan yang ditetapkan oleh organisasi maupun regulasi pemerintah.

Dalam prakteknya, kontrol dan audit teknologi informasi saling melengkapi satu sama lain. Kontrol teknologi informasi memastikan bahwa sistem dan data teknologi informasi dalam suatu organisasi terlindungi dengan baik, sementara audit teknologi informasi memastikan bahwa kontrol tersebut efektif dan efisien dalam menjaga keamanan dan keandalan sistem dan data tersebut.

5.2 Hal – hal Penting Dalam Audit Perangkat Keras

Teknik audit perangkat keras melibatkan pemeriksaan perangkat keras komputer dan perangkat yang terkait, termasuk jaringan, server, dan perangkat penyimpanan data. Berikut adalah beberapa teknik audit perangkat keras yang baik: (Tumanggor and Adriansyah, 2021)

1. Identifikasi dan penilaian risiko: Sebelum melakukan audit perangkat keras, auditor perlu mengidentifikasi dan mengevaluasi risiko keamanan dan kerentanan sistem. Hal ini meliputi pemahaman terhadap kerentanan dan ancaman yang mungkin terjadi pada sistem, serta potensi dampak keamanan yang mungkin terjadi jika terjadi pelanggaran keamanan.
2. Pemeriksaan fisik perangkat keras: Auditor perlu melakukan pemeriksaan fisik perangkat keras untuk memastikan bahwa perangkat keras yang digunakan dalam organisasi memenuhi standar keamanan yang ditetapkan. Ini meliputi pemeriksaan koneksi kabel, slot kartu, dan perangkat keras lainnya untuk memastikan bahwa semuanya terpasang dengan benar dan tidak ada yang rusak.

3. Pemeriksaan konfigurasi sistem: Auditor perlu memeriksa konfigurasi sistem untuk memastikan bahwa sistem diatur dengan benar dan memenuhi standar keamanan. Ini meliputi pemeriksaan konfigurasi jaringan, server, dan perangkat penyimpanan data.
4. Pemeriksaan tata kelola IT: Auditor perlu memeriksa tata kelola IT organisasi untuk memastikan bahwa proses dan kebijakan keamanan diatur dengan benar dan sesuai dengan standar keamanan. Hal ini meliputi pemeriksaan kebijakan akses, tata kelola perangkat keras, dan tata kelola keamanan sistem.
5. Pemeriksaan dokumentasi dan catatan: Auditor perlu memeriksa dokumentasi dan catatan untuk memastikan bahwa seluruh perangkat keras dan sistem yang digunakan dalam organisasi telah didokumentasikan dengan baik. Ini meliputi pemeriksaan dokumentasi dan catatan penggunaan perangkat keras, sertifikat keamanan, dan dokumentasi konfigurasi sistem.
6. Penilaian penggunaan teknologi baru: Auditor perlu memperhatikan teknologi baru yang digunakan dalam organisasi dan mengevaluasi apakah teknologi tersebut memenuhi standar keamanan dan keandalan yang ditetapkan.
7. Pengujian keamanan perangkat keras: Auditor perlu melakukan pengujian keamanan pada perangkat keras untuk memastikan bahwa sistem tidak rentan terhadap serangan yang mengancam keamanan. Hal ini meliputi pengujian penetrasi dan pengujian serangan yang mungkin terjadi pada sistem.
8. Pemantauan aktivitas pengguna: Auditor perlu memeriksa keamanan aktivitas pengguna dalam sistem untuk memastikan bahwa tidak ada aktivitas yang mencurigakan atau melanggar kebijakan keamanan yang ditetapkan. Ini

meliputi pemeriksaan log aktivitas pengguna dan pengujian keamanan terhadap akses pengguna pada sistem.

9. Evaluasi kualitas pemeliharaan: Auditor perlu mengevaluasi kualitas pemeliharaan perangkat keras dan sistem. Ini meliputi pemeriksaan pemeliharaan rutin, patching, pembaruan, dan penggantian perangkat keras yang sudah usang. Pemeliharaan yang buruk dapat mengakibatkan sistem menjadi rentan terhadap ancaman keamanan.
10. Penilaian kebijakan backup dan recovery: Auditor perlu mengevaluasi kebijakan backup dan recovery yang ditetapkan oleh organisasi untuk memastikan bahwa sistem dan data yang dihasilkan oleh sistem terlindungi dan dapat dipulihkan jika terjadi kehilangan atau kerusakan. Ini meliputi penilaian prosedur backup dan recovery, pengujian proses restore data, dan kebijakan penjagaan data backup.
11. Pengujian dan verifikasi penghapusan data: Auditor perlu memeriksa proses penghapusan data untuk memastikan bahwa data yang dihapus benar-benar tidak lagi dapat diakses. Hal ini penting untuk mencegah data sensitif atau rahasia terbocor ke publik atau pihak yang tidak berwenang.
12. Pemeriksaan penggunaan teknologi enkripsi: Auditor perlu mengevaluasi penggunaan teknologi enkripsi dalam sistem untuk memastikan bahwa data yang dihasilkan oleh sistem terlindungi dengan baik. Ini meliputi pemeriksaan penggunaan teknologi enkripsi untuk data yang sensitif dan proses enkripsi yang dilakukan pada data dalam sistem.
13. Memperhatikan kondisi fisik perangkat keras: Auditor perlu memeriksa kondisi fisik perangkat keras untuk

memastikan bahwa tidak ada kerusakan atau cacat pada perangkat keras. Hal ini meliputi pemeriksaan kondisi fisik perangkat keras seperti keyboard, mouse, monitor, printer, server, dan komputer.

14. Memeriksa proses pemasangan dan konfigurasi: Auditor perlu memeriksa proses pemasangan dan konfigurasi perangkat keras untuk memastikan bahwa dilakukan secara benar dan sesuai dengan standar keamanan dan keandalan yang ditetapkan.
15. Memeriksa keberadaan dan keamanan kabel jaringan: Auditor perlu memeriksa keberadaan dan keamanan kabel jaringan untuk memastikan bahwa tidak ada kabel yang terputus atau terpengaruh oleh interferensi elektromagnetik atau gangguan lainnya.
16. Memeriksa penggunaan perangkat lunak: Auditor perlu memeriksa penggunaan perangkat lunak yang terinstall pada perangkat keras untuk memastikan bahwa perangkat lunak yang digunakan adalah legal dan telah dilisensi secara benar.
17. Memeriksa penggunaan perangkat keras tambahan: Auditor perlu memeriksa penggunaan perangkat keras tambahan seperti USB drive, kartu memori, atau perangkat penyimpanan lainnya untuk memastikan bahwa perangkat tambahan yang digunakan aman dan tidak membahayakan sistem.
18. Memeriksa penggunaan perangkat keras oleh pengguna: Auditor perlu memeriksa penggunaan perangkat keras oleh pengguna untuk memastikan bahwa pengguna telah mendapatkan pelatihan yang cukup dan mengikuti prosedur keamanan yang ditetapkan.
19. Memeriksa prosedur penanganan kerusakan: Auditor perlu memeriksa prosedur penanganan kerusakan pada perangkat keras untuk memastikan bahwa prosedur

tersebut efektif dan dapat mengurangi downtime pada sistem.

20. Memeriksa kebijakan keamanan informasi: Auditor perlu memeriksa kebijakan keamanan informasi yang ditetapkan oleh organisasi untuk memastikan bahwa kebijakan tersebut memenuhi standar keamanan yang berlaku. Hal ini meliputi pemeriksaan kebijakan tentang password, akses, dan penggunaan sistem.
21. Memeriksa kepatuhan terhadap standar keamanan: Auditor perlu memeriksa kepatuhan organisasi terhadap standar keamanan yang berlaku seperti ISO 27001, PCI DSS, atau standar keamanan lainnya yang sesuai dengan industri organisasi tersebut. Hal ini meliputi pemeriksaan terhadap kepatuhan terhadap standar keamanan yang ditetapkan oleh badan regulasi atau organisasi yang berkaitan.
22. Memeriksa sistem monitoring dan deteksi intrusi: Auditor perlu memeriksa sistem monitoring dan deteksi intrusi yang digunakan oleh organisasi untuk memastikan bahwa sistem tersebut berfungsi dengan baik dan dapat mendeteksi ancaman keamanan dengan cepat.
23. Memeriksa sistem firewall dan filter akses: Auditor perlu memeriksa sistem firewall dan filter akses yang digunakan oleh organisasi untuk memastikan bahwa sistem tersebut telah dikonfigurasi dengan benar dan dapat melindungi sistem dari ancaman luar.
24. Memeriksa sistem enkripsi dan dekripsi: Auditor perlu memeriksa sistem enkripsi dan dekripsi yang digunakan oleh organisasi untuk memastikan bahwa data yang sensitif telah terenkripsi dengan baik dan tidak dapat diakses oleh pihak yang tidak berwenang.
25. Memeriksa sistem backup dan recovery: Auditor perlu memeriksa sistem backup dan recovery yang digunakan

oleh organisasi untuk memastikan bahwa sistem dan data yang dihasilkan oleh sistem terlindungi dan dapat dipulihkan jika terjadi kehilangan atau kerusakan.

26. Memeriksa kebijakan dan prosedur manajemen risiko: Auditor perlu memeriksa kebijakan dan prosedur manajemen risiko yang digunakan oleh organisasi untuk mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi yang mungkin terjadi. Hal ini meliputi pemeriksaan terhadap kebijakan dan prosedur yang digunakan untuk mengidentifikasi dan mengevaluasi risiko, serta strategi untuk mengelola risiko yang telah diidentifikasi.
27. Memeriksa sistem pengelolaan identitas dan akses: Auditor perlu memeriksa sistem pengelolaan identitas dan akses yang digunakan oleh organisasi untuk memastikan bahwa hak akses pengguna telah dikonfigurasi dengan benar dan tidak terjadi pelanggaran terhadap privasi atau keamanan informasi.
28. Memeriksa sistem pengendalian akses fisik: Auditor perlu memeriksa sistem pengendalian akses fisik yang digunakan oleh organisasi untuk memastikan bahwa hanya orang yang berwenang yang dapat mengakses sistem dan informasi yang sensitif.
29. Memeriksa keamanan jaringan: Auditor perlu memeriksa keamanan jaringan yang digunakan oleh organisasi untuk memastikan bahwa jaringan telah terproteksi dengan baik dan tidak rentan terhadap serangan jaringan.
30. Memeriksa kebijakan dan prosedur manajemen keamanan informasi: Auditor perlu memeriksa kebijakan dan prosedur manajemen keamanan informasi yang digunakan oleh organisasi untuk memastikan bahwa sistem dan informasi terproteksi dengan baik dan terkelola dengan benar.

Melalui teknik audit perangkat keras yang baik, auditor dapat membantu organisasi untuk memastikan bahwa perangkat keras dan sistem mereka aman dan andal.

Dalam melakukan audit perangkat keras, auditor perlu memperhatikan faktor-faktor tersebut dan melakukan pengujian secara komprehensif untuk memastikan bahwa sistem dan perangkat keras yang digunakan oleh organisasi memenuhi standar keamanan dan keandalan yang ditetapkan.
Dalam melakukan audit perangkat keras yang baik, auditor juga harus memastikan bahwa prosedur audit dilakukan secara teratur dan sesuai dengan standar audit yang ditetapkan. Dengan demikian, auditor dapat memastikan bahwa perangkat keras yang digunakan oleh organisasi aman dan dapat diandalkan dalam menjalankan operasinya.

Dalam melakukan audit keamanan informasi, auditor perlu memastikan bahwa sistem dan kebijakan keamanan informasi yang digunakan oleh organisasi memenuhi standar keamanan dan dapat melindungi sistem dari ancaman keamanan. Oleh karena itu, auditor harus memperhatikan faktor-faktor tersebut dan melakukan pengujian secara komprehensif untuk memastikan bahwa sistem dan perangkat keras yang digunakan oleh organisasi aman dan dapat diandalkan dalam menjalankan operasinya.

Dalam melakukan audit perangkat keras, auditor harus memastikan bahwa organisasi telah menerapkan kebijakan dan prosedur yang memadai untuk melindungi perangkat keras dan data yang terdapat di dalamnya. Selain itu, auditor juga harus memeriksa sistem dan infrastruktur teknologi informasi yang digunakan oleh organisasi dan memastikan bahwa sistem tersebut telah terproteksi dengan baik dan memenuhi standar keamanan yang berlaku.

5.3 Perangkat Keras Komputer

Berikut ini adalah beberapa jenis perangkat keras komputer:

1. CPU (*Central Processing Unit*): adalah komponen inti dari sebuah komputer yang berfungsi sebagai otak dari sistem. CPU bertanggung jawab untuk mengatur dan mengeksekusi instruksi-instruksi program yang terdapat pada sistem komputer.
2. RAM (*Random Access Memory*): adalah perangkat keras yang digunakan untuk menyimpan data sementara dan memberikan ruang kerja bagi CPU dalam mengeksekusi program.
3. *Hard Disk Drive* (HDD): adalah perangkat keras yang digunakan untuk menyimpan data secara permanen. HDD biasanya digunakan untuk menyimpan sistem operasi, aplikasi, dan data pengguna.
4. *Solid State Drive* (SSD): adalah jenis hard disk drive yang menggunakan teknologi flash memory untuk menyimpan data. SSD biasanya memiliki performa yang lebih baik dan lebih awet dibandingkan HDD.
5. *Motherboard*: adalah papan sirkuit utama yang menghubungkan semua komponen perangkat keras di dalam komputer.
6. *Power Supply Unit* (PSU): adalah perangkat keras yang bertanggung jawab untuk menyediakan daya listrik yang diperlukan oleh semua komponen perangkat keras di dalam komputer.
7. Kartu Grafis: adalah perangkat keras yang digunakan untuk menghasilkan tampilan grafis pada layar komputer. Kartu grafis digunakan untuk memainkan game atau bekerja dengan aplikasi grafis.
8. *Sound Card*: adalah perangkat keras yang digunakan untuk memproses suara pada komputer. Sound card biasanya

digunakan untuk mendengarkan musik, berbicara melalui telepon internet, atau bermain game.

9. *Monitor*: adalah perangkat keras yang digunakan untuk menampilkan output dari komputer. Monitor biasanya berupa layar datar (*flat screen*) yang terhubung ke CPU melalui kabel VGA, HDMI atau DisplayPort.
10. *Keyboard dan Mouse*: adalah perangkat keras yang digunakan untuk menginput data dan mengendalikan komputer. Keyboard biasanya digunakan untuk mengetik teks dan perintah, sementara mouse digunakan untuk menggerakkan kursor pada layar dan memilih opsi yang diinginkan.
11. *Printer:* adalah perangkat keras yang digunakan untuk mencetak dokumen dan gambar dari komputer. Printer biasanya terhubung ke CPU melalui USB atau jaringan.
12. *Scanner:* adalah perangkat keras yang digunakan untuk memindai dokumen atau gambar menjadi file digital. Scanner biasanya terhubung ke CPU melalui USB atau jaringan.

Itulah beberapa jenis perangkat keras komputer yang umum digunakan pada sistem komputer modern.

5.4 Perangkat Keras Infrastruktur

Berikut ini adalah beberapa jenis perangkat keras infrastruktur (*networking)* yang digunakan dalam sistem komunikasi jaringan:

1. Router: adalah perangkat keras yang menghubungkan dua atau lebih jaringan dan mampu meneruskan paket data antara jaringan tersebut.
2. *Switch*: adalah perangkat keras yang digunakan untuk menghubungkan beberapa perangkat di jaringan lokal

(LAN) dan meneruskan paket data antar perangkat tersebut.

3. *Firewall*: adalah perangkat keras yang digunakan untuk melindungi jaringan dari serangan luar, seperti serangan hacking dan virus.
4. *Access Point*: adalah perangkat keras yang digunakan untuk menghubungkan perangkat nirkabel ke jaringan kabel.
5. *Network Interface Card* (NIC): adalah perangkat keras yang digunakan untuk menghubungkan komputer atau server ke jaringan kabel.
6. Modem: adalah perangkat keras yang digunakan untuk mengubah sinyal digital menjadi sinyal analog dan sebaliknya, sehingga memungkinkan komputer untuk terhubung ke internet melalui jaringan telepon atau kabel TV.
7. Hub: adalah perangkat keras yang digunakan untuk menghubungkan beberapa perangkat di jaringan lokal (LAN) dan meneruskan paket data antar perangkat tersebut.
8. Repeater: adalah perangkat keras yang digunakan untuk memperpanjang jarak jangkauan sinyal dalam jaringan.
9. Bridge: adalah perangkat keras yang digunakan untuk menghubungkan dua jaringan lokal (LAN) yang berbeda dan meneruskan paket data antar jaringan tersebut.
10. *Gateway*: adalah perangkat keras yang digunakan untuk menghubungkan dua atau lebih jaringan yang berbeda dan memungkinkan perpindahan data antara jaringan tersebut.
11. *Load balancer*: adalah perangkat keras yang digunakan untuk mendistribusikan lalu lintas jaringan secara merata ke beberapa server, sehingga mengoptimalkan kinerja jaringan.

Itulah beberapa jenis perangkat keras infrastruktur (*networking*) yang umum digunakan pada sistem komunikasi jaringan modern.

5.5 Tujuan Audit Perangkat Keras

Tujuan audit perangkat keras adalah untuk memastikan bahwa perangkat keras yang digunakan oleh organisasi atau perusahaan telah diatur dengan baik, berfungsi secara efektif, dan dapat dipercaya. Beberapa tujuan khusus dari audit perangkat keras antara lain: (Rasheed, 2014)

1. Memastikan bahwa perangkat keras yang digunakan oleh organisasi atau perusahaan memenuhi standar dan spesifikasi yang ditentukan.
2. Memastikan bahwa perangkat keras yang digunakan telah diinstal dan dikonfigurasi dengan benar sehingga dapat beroperasi secara efektif.
3. Memastikan bahwa perangkat keras yang digunakan telah dilindungi dari risiko keamanan dan telah diatur dengan sistem manajemen risiko yang tepat.
4. Memastikan bahwa perangkat keras yang digunakan telah dikelola dan diawasi dengan baik agar dapat terus berfungsi secara optimal dan dapat diandalkan.
5. Memastikan bahwa organisasi atau perusahaan telah menjalankan prosedur perawatan dan perbaikan yang tepat untuk perangkat keras yang digunakan, sehingga dapat memperpanjang umur perangkat keras dan mengurangi risiko kegagalan.
6. Mengevaluasi efisiensi dan efektivitas penggunaan perangkat keras dan memastikan bahwa organisasi atau perusahaan mengalokasikan sumber daya dengan benar untuk perangkat keras dan infrastruktur teknologi informasi yang diperlukan.

7. Memastikan bahwa kebijakan dan prosedur yang diterapkan untuk penggunaan perangkat keras sudah sesuai dengan standar dan peraturan terkait.
8. Memastikan bahwa perangkat keras yang digunakan oleh organisasi atau perusahaan telah melalui pengujian yang memadai dan tidak mengandung cacat atau kerusakan yang dapat menyebabkan masalah.
9. Menilai tingkat keamanan perangkat keras dan mengidentifikasi risiko keamanan yang terkait dengan penggunaan perangkat keras.
10. Memberikan rekomendasi untuk perbaikan dan peningkatan penggunaan perangkat keras yang dapat membantu organisasi atau perusahaan dalam mengurangi risiko dan meningkatkan efisiensi dan efektivitas penggunaan perangkat keras.

Dengan melakukan audit perangkat keras secara teratur, organisasi atau perusahaan dapat memastikan bahwa perangkat keras yang digunakan telah diatur dengan baik dan berfungsi secara efektif. Hal ini juga dapat membantu organisasi atau perusahaan dalam mengidentifikasi risiko dan memperbaiki masalah yang mungkin terjadi pada perangkat keras sehingga dapat mengurangi kerugian dan meningkatkan efisiensi dan efektivitas operasional.

5.6 Persiapan Audit Perangkat Keras

Berikut ini adalah beberapa hal penting yang harus dipersiapkan untuk memenuhi standar audit perangkat keras:

1. Memiliki daftar inventaris perangkat keras yang dimiliki oleh organisasi atau perusahaan, termasuk jenis, merek, model, dan spesifikasi perangkat keras tersebut.
2. Memiliki kebijakan dan prosedur pengadaan perangkat keras yang sesuai dengan standar dan peraturan terkait.

3. Memiliki kebijakan dan prosedur penggunaan perangkat keras yang sesuai dengan standar dan peraturan terkait.
4. Memiliki kebijakan dan prosedur perawatan perangkat keras yang sesuai dengan standar dan peraturan terkait.
5. Memiliki kebijakan dan prosedur pemindaian dan pengujian perangkat keras untuk mendeteksi kerentanan atau kelemahan yang mungkin dieksploitasi oleh pihak yang tidak bertanggung jawab.
6. Memiliki kebijakan dan prosedur pemantauan dan pengelolaan keamanan perangkat keras yang sesuai dengan standar dan peraturan terkait.
7. Memiliki dokumentasi tentang pemeliharaan dan perbaikan perangkat keras yang dilakukan oleh teknisi atau pihak yang ditunjuk.
8. Memiliki kontrol akses fisik ke perangkat keras yang penting, seperti server dan pusat data, yang hanya diizinkan untuk diakses oleh orang-orang yang berwenang.
9. Melakukan pemantauan terhadap perangkat keras yang digunakan untuk mendeteksi masalah atau kerusakan yang mungkin terjadi.
10. Menyimpan arsip pemeliharaan dan perbaikan perangkat keras untuk tujuan audit dan verifikasi.
11. Melakukan pelatihan dan sertifikasi untuk teknisi dan personel yang terlibat dalam perawatan, perbaikan, dan pengelolaan perangkat keras.
12. Memiliki kebijakan dan prosedur yang memastikan bahwa perangkat keras yang tidak lagi digunakan atau sudah usang tidak dipakai atau dijual kembali tanpa dihapus data sensitif yang tersimpan di dalamnya.
13. Melakukan pemeriksaan keamanan secara berkala untuk memastikan bahwa konfigurasi perangkat keras dan perangkat lunak yang digunakan tetap aman dan tidak

terdapat celah yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab.

14. Memiliki prosedur pemulihan bencana untuk perangkat keras yang penting, seperti server, untuk memastikan bahwa data dapat dipulihkan dengan cepat dalam situasi darurat.
15. Melakukan pengujian keandalan dan kinerja perangkat keras secara berkala untuk memastikan bahwa perangkat keras yang digunakan berfungsi secara optimal dan tidak mengalami masalah yang dapat mempengaruhi kinerja atau produktivitas organisasi atau perusahaan.
16. Menyimpan backup data secara teratur dan melakukan pemulihan data jika terjadi kerusakan atau kehilangan data pada perangkat keras.

Dengan mempersiapkan hal-hal tersebut, organisasi atau perusahaan dapat memenuhi standar audit perangkat keras dan meningkatkan efektivitas dan efisiensi penggunaan perangkat keras secara keseluruhan. Hal ini juga dapat membantu organisasi atau perusahaan dalam mengidentifikasi risiko keamanan dan mengurangi kemungkinan terjadinya gangguan atau kerusakan pada perangkat keras.

5.7 Orang yang Terlibat didalam Audit Perangkat Keras

Berikut adalah beberapa orang yang terlibat dalam audit perangkat keras:

1. Auditor: Auditor adalah orang yang bertanggung jawab melakukan audit perangkat keras. Auditor harus memiliki pengetahuan dan keterampilan yang memadai dalam melakukan audit perangkat keras, termasuk pemahaman tentang spesifikasi perangkat keras, standar audit, keamanan perangkat keras, dan alat audit perangkat keras.

2. Manajer IT: Manajer IT adalah orang yang bertanggung jawab atas pengelolaan sistem informasi dan perangkat keras yang digunakan oleh organisasi atau perusahaan. Manajer IT biasanya terlibat dalam pengambilan keputusan tentang pengadaan, penggunaan, dan perawatan perangkat keras, sehingga kehadiran mereka dalam audit perangkat keras sangat penting.
3. Teknisi perangkat keras: Teknisi perangkat keras adalah orang yang bertanggung jawab atas pemeliharaan, perbaikan, dan pengelolaan perangkat keras. Mereka harus memiliki pengetahuan dan keterampilan yang memadai dalam melakukan pemeliharaan dan perbaikan perangkat keras, serta memahami standar dan kebijakan yang berlaku terkait pengelolaan perangkat keras.
4. Tim keamanan IT: Tim keamanan IT bertanggung jawab atas memastikan keamanan perangkat keras dan sistem informasi organisasi atau perusahaan. Mereka harus memahami risiko keamanan yang terkait dengan penggunaan perangkat keras dan memastikan bahwa perangkat keras dan sistem informasi dilindungi dengan baik.
5. Pengguna perangkat keras: Pengguna perangkat keras adalah orang yang menggunakan perangkat keras dalam kegiatan sehari-hari. Pengguna perangkat keras harus mematuhi kebijakan dan prosedur terkait penggunaan perangkat keras yang telah ditetapkan oleh organisasi atau perusahaan, serta melaporkan masalah atau kerusakan perangkat keras yang mereka temukan.
6. Manajemen senior: Manajemen senior bertanggung jawab atas pengambilan keputusan strategis dan pengelolaan risiko organisasi atau perusahaan. Kehadiran mereka dalam audit perangkat keras dapat membantu memastikan bahwa pengelolaan perangkat keras dan sistem informasi

dilakukan dengan benar dan sesuai dengan tujuan organisasi atau perusahaan.

7. Pihak ketiga: Pihak ketiga, seperti vendor perangkat keras atau penyedia layanan perangkat keras, juga dapat terlibat dalam audit perangkat keras. Pihak ketiga harus dapat memberikan informasi yang diperlukan terkait dengan spesifikasi perangkat keras dan kebijakan perawatan perangkat keras yang diterapkan oleh organisasi atau perusahaan.
8. Auditor internal: Auditor internal bertanggung jawab atas audit internal di dalam organisasi atau perusahaan. Auditor internal dapat membantu dalam melaksanakan audit perangkat keras dengan memberikan informasi terkait dengan sistem informasi dan perangkat keras yang digunakan di organisasi atau perusahaan.
9. Auditor eksternal: Auditor eksternal adalah auditor yang dipekerjakan dari luar organisasi atau perusahaan untuk melakukan audit. Auditor eksternal dapat memberikan pandangan independen terhadap audit perangkat keras dan membantu memastikan bahwa audit dilakukan dengan objektif dan adil.
10. Regulator: Regulator bertanggung jawab atas memastikan bahwa organisasi atau perusahaan mematuhi standar dan peraturan yang berlaku. Regulator dapat memeriksa audit perangkat keras yang dilakukan oleh organisasi atau perusahaan untuk memastikan bahwa organisasi atau perusahaan telah memenuhi standar dan peraturan yang berlaku.
11. Pengembang perangkat keras: Pengembang perangkat keras bertanggung jawab atas merancang dan mengembangkan perangkat keras. Kehadiran pengembang perangkat keras dalam audit perangkat keras dapat membantu memberikan informasi tentang spesifikasi

perangkat keras dan kebijakan perawatan perangkat keras yang dapat membantu dalam audit.

12. Pengacara: Pengacara dapat terlibat dalam audit perangkat keras untuk memberikan pandangan hukum terkait dengan kebijakan dan prosedur pengelolaan perangkat keras, serta risiko hukum yang terkait dengan keamanan dan privasi data.
13. Pemilik bisnis: Pemilik bisnis bertanggung jawab atas pengambilan keputusan bisnis dan memastikan bahwa penggunaan perangkat keras mendukung tujuan bisnis organisasi atau perusahaan. Kehadiran pemilik bisnis dalam audit perangkat keras dapat membantu dalam memastikan bahwa audit perangkat keras mencerminkan kebutuhan bisnis dan memastikan bahwa penggunaan perangkat keras mendukung tujuan bisnis.
14. Tim audit internal: Tim audit internal bertanggung jawab atas audit internal di dalam organisasi atau perusahaan. Tim audit internal dapat membantu dalam melaksanakan audit perangkat keras dengan memberikan informasi terkait dengan sistem informasi dan perangkat keras yang digunakan di organisasi atau perusahaan.
15. Penasihat keamanan: Penasihat keamanan adalah ahli keamanan yang bertanggung jawab atas memastikan bahwa organisasi atau perusahaan memiliki strategi keamanan yang tepat. Penasihat keamanan dapat membantu dalam audit perangkat keras dengan memberikan informasi tentang risiko keamanan yang terkait dengan penggunaan perangkat keras dan membantu dalam menentukan tindakan pengamanan yang tepat untuk melindungi perangkat keras dan sistem informasi dari ancaman keamanan.

5.8 Penyebab Kegagalan Audit Perangkat Keras

Kegagalan audit perangkat keras dapat terjadi karena berbagai alasan, di antaranya:

1. Ketidakmampuan auditor untuk mengidentifikasi masalah: Auditor mungkin tidak memiliki pengetahuan atau pengalaman yang cukup dalam memeriksa perangkat keras, sehingga mereka tidak dapat mengidentifikasi masalah yang terkait.
2. Kurangnya akses: Auditor mungkin tidak diberikan akses yang cukup ke perangkat keras yang akan diaudit, sehingga mereka tidak dapat memeriksanya dengan benar.
3. Kesalahan manusia: Kegagalan audit perangkat keras juga dapat terjadi karena kesalahan manusia, seperti kesalahan dalam proses pengujian atau kesalahan dalam interpretasi hasil pengujian.
4. Kegagalan perangkat keras: Perangkat keras itu sendiri dapat mengalami kegagalan atau kerusakan yang mengakibatkan audit tidak berhasil.
5. Kecurangan: Ada kemungkinan bahwa kegagalan audit perangkat keras terjadi karena adanya kecurangan atau manipulasi oleh pihak yang di-audit untuk menghindari pengungkapan masalah yang sebenarnya.

Untuk menghindari kegagalan audit perangkat keras, ada beberapa langkah yang dapat diambil:

1. Memilih auditor yang kompeten dan berpengalaman dalam melakukan audit perangkat keras.
2. Memberikan akses yang cukup kepada auditor untuk memeriksa perangkat keras yang akan diaudit.
3. Menjalankan proses audit dengan benar dan hati-hati, termasuk dalam pengujian dan interpretasi hasil pengujian.
4. Memastikan bahwa perangkat keras yang akan diaudit dalam kondisi yang baik dan berfungsi dengan benar.

5. Membuat laporan audit yang jelas dan terperinci, mencakup hasil pengujian dan temuan serta rekomendasi untuk memperbaiki masalah yang ditemukan.
6. Melakukan tindakan perbaikan dan tindak lanjut untuk memastikan bahwa masalah yang ditemukan selama audit diperbaiki dan tidak terulang kembali di masa depan.
7. Menjaga integritas dan transparansi dalam proses audit, dan tidak mengizinkan adanya kecurangan atau manipulasi dalam pengungkapan hasil audit.

Selain langkah-langkah tersebut, ada beberapa hal yang dapat dilakukan untuk meminimalkan risiko kegagalan audit perangkat keras, di antaranya:

1. Memiliki prosedur audit yang terstandarisasi dan terdokumentasi dengan baik. Prosedur audit yang jelas dan terstandarisasi akan memudahkan auditor dalam menjalankan audit dan mengurangi risiko kesalahan atau kekurangan dalam proses audit.
2. Melakukan pemeriksaan perangkat keras secara berkala untuk memastikan bahwa perangkat keras tersebut tetap berfungsi dengan baik dan sesuai dengan kebutuhan bisnis.
3. Memiliki kontrak atau perjanjian audit yang jelas dengan auditor, termasuk hak dan tanggung jawab masing-masing pihak dalam proses audit.
4. Melakukan audit internal secara rutin untuk memastikan bahwa sistem kontrol internal dalam organisasi bekerja dengan baik dan memenuhi standar audit.
5. Mengikuti praktik terbaik dalam manajemen perangkat keras, termasuk dalam pemilihan dan penggunaan perangkat keras yang sesuai untuk kebutuhan bisnis dan penggunaannya secara aman dan teratur.

Dengan melakukan langkah-langkah ini, organisasi dapat meminimalkan risiko kegagalan audit perangkat keras dan memastikan bahwa perangkat keras mereka bekerja dengan baik dan sesuai dengan kebutuhan bisnis.

DAFTAR PUSTAKA

Rasheed, H. 2014. 'Data and infrastructure security auditing in cloud computing environments', *International Journal of Information Management*, 34(3), pp. 364–368. Available at: https://doi.org/10.1016/j.ijinfomgt.2013.11.002.

Tumanggor, A.H. and Adriansyah, T. 2021. 'Dampak Teknologi Informasi Terhadap Audit Internal', *Juripol (Jurnal Institusi Politeknik Ganesha Medan)*, 3(2), pp. 8–18. Available at: https://doi.org/10.33395/juripol.v3i2.10865.

BAB 6
TEKNIK AUDIT PERANGKAT LUNAK

Oleh Rima Rizqi Wijayanti

6.1 Pendahuluan

Saat ini, mayoritas perusahaan menggunakan berbagai alat dan aplikasi digital yang dapat membentuk ekosistem perangkat lunak pada perusahaan. Dari waktu ke waktu, ada kebutuhan untuk menjalankan audit untuk melihat apakah semuanya sebagaimana mestinya, dilihat dari sudut pandang hukum, operasional, dan eksploitasi. Dan karena perangkat lunak sekarang sering kali merupakan bagian penting dalam kegiatan suatu perusahaan, maka audit perangkat lunak menjadi sangat penting untuk menjamin keberlangsungan proses bisnis pada suatu organisasi(Otero, 2019).

6.2 Apa itu audit perangkat lunak?

Audit perangkat lunak, pada kenyataannya, adalah istilah yang sangat luas. Ini dapat berhubungan dengan sesuatu yang dilakukan perusahaan secara internal atau eksternal (oleh auditor pihak ketiga). Secara umum, ini adalah prosedur yang bertujuan untuk memverifikasi keadaan, kualitas, dan kepatuhan perangkat lunak yang digunakan dalam organisasi tertentu(Gillis, 2022).

Audit perangkat lunak adalah tinjauan internal atau eksternal dari program perangkat lunak untuk memeriksa kualitas, kemajuan, atau kepatuhannya terhadap rencana,

standar, dan peraturan. Proses ini dilakukan oleh tim internal atau oleh satu atau lebih auditor independen.

Terkadang audit perangkat lunak dilakukan karena alasan hukum (misalnya untuk memverifikasi bahwa ada lisensi yang cukup untuk mencakup penggunaan perangkat lunak, seperti dalam audit hak cipta perangkat lunak), atau untuk memastikan staf menggunakan versi perangkat lunak yang sama, atau untuk memastikan bahwa tidak ada kelebihan lisensi.

Beberapa alasan paling umum untuk melakukan audit perangkat lunak adalah, misalnya:

1. Menemukan potensi masalah dan gangguan yang perlu diperbaiki
2. Pelacakan penggunaan perangkat lunak (misalnya, untuk mengetahui program dan aplikasi apa yang tidak digunakan atau ketinggalan zaman), termasuk frekuensi dan siapa yang menggunakan perangkat lunak;
3. untuk memantau jaminan kualitas (QA);
4. Memverifikasi kepatuhan lisensi (audit lisensi perangkat lunak)
5. Memverifikasi apakah perangkat lunak Anda memenuhi semua persyaratan hukum (misalnya, mengenai pemrosesan data pribadi) dan untuk mematuhi standar industri.

Seperti yang disebutkan, ada audit perangkat lunak internal dan eksternal. Tim internal biasanya berkonsentrasi pada keadaan dan kualitas perangkat lunak Anda. Sedangkan Audit eksternal dilakukan oleh auditor pihak ketiga yang tidak perlu memihak dan memeriksa semuanya sesuai dengan prosedur mereka. Audit perangkat lunak semacam itu biasanya berfokus pada potensi masalah kepatuhan dan hukum. Alih-alih berfokus pada kualitas teknis perangkat lunak, audit perangkat

lunak berfokus pada kepatuhan produk atau proses. Hal ini merupakan bagian penting dalam mengevaluasi apakah produk atau proses perangkat lunak mematuhi peraturan, standar, dan prosedur.

Audit perangkat lunak melayani tujuan penting bagi suatu organisasi. Tetapi juga dapat mengganggu perkembangan perusahaan dan dapat menempatkan tekanan keuangan pada suatu proyek karena jika biaya audit tidak dianggarkan. Tim dan manajemen mungkin diminta untuk berkonsultasi dengan auditor untuk memastikan prosesnya lengkap dan akurat. Konsultasi yang terlibat dapat menghilangkan waktu yang dihabiskan untuk bekerja. Organisasi harus menahan diri dari audit yang berlebihan, dan eksekutif harus memahami bagaimana, mengapa dan kapan audit dilakukan sehingga mereka dapat mempersiapkannya dengan sebaik-baiknya.

6.3 Mengapa audit perangkat lunak diperlukan?

Proses audit perangkat lunak diperlukan karena beberapa alasan.

Pertama-tama, ini membantu kita dalam memelihara semua perangkat lunak dalam kondisi sehat. Aplikasi dan program sering diperbarui dan dimodifikasi. Setiap versi baru dilengkapi dengan tweak yang berguna, misalnya, mengenai keamanan siber. Adalah kepentingan terbaik Anda untuk memastikan bahwa semua program yang Anda gunakan efektif dan aman.

Kedua, masalah perizinan. Mayoritas aplikasi perusahaan memerlukan lisensi untuk menggunakannya secara legal. Dan setiap lisensi tersebut menghasilkan biaya setiap tahun. Jika ada aplikasi yang tidak lagi digunakan perusahaan Anda (atau yang dapat dengan mudah diganti dengan alternatif yang lebih murah), audit semacam itu dapat menghemat banyak uang.

Terakhir, kami memiliki audit perangkat lunak kegunaan. Mereka berguna ketika Anda mengembangkan perangkat lunak Anda sendiri dan ingin memastikan bahwa itu berfungsi penuh dan intuitif untuk digunakan, bahkan untuk pengguna yang kurang paham teknologi. Kunci keberhasilan terletak pada pemilihan audit yang diperlukan dengan hati-hati yang Anda rasa perlu dan akan membantu Anda meningkatkan cara kerja organisasi Anda.

Audit internal dapat membantu organisasi meningkatkan efisiensinya dengan mengurangi jumlah lisensi yang tidak aktif atau kedaluwarsa dan menemukan masalah sebelum dapat menjadi masalah lisensi atau peraturan dalam tinjauan pihak ketiga. Tinjauan eksternal, atau pihak ketiga, umumnya berfokus pada perangkat lunak yang digunakan di luar hak berlisensi dan dapat membantu mengidentifikasi kesenjangan kepatuhan. Prioritas yang berbeda ini berarti adalah bijaksana bagi organisasi untuk melakukan tinjauan internal sebelum audit eksternal.

Jika audit internal dilakukan, auditor yang dipilih organisasi harus independen dan tidak memihak. Auditor kemudian menentukan apakah ada pelanggaran seperti pembajakan. Misalnya, organisasi mungkin telah membeli satu lisensi perangkat lunak tetapi menginstal salinan perangkat lunak pada beberapa perangkat.

Secara internal, audit perangkat lunak membantu organisasi mendapatkan pemeriksaan realitas tentang keadaan mereka saat ini seputar penggunaan perangkat lunak. Audit dapat membantu memastikan perangkat lunak yang digunakan organisasi adalah yang terbaru dan berfungsi sebagaimana mestinya.

Audit perangkat lunak dilakukan ketika organisasi percaya bahwa itu mungkin melanggar perjanjian penggunanya. Organisasi dapat memulai audit perangkat lunak

ketika kepatuhan lisensi perlu diverifikasi, untuk memantau QA, untuk memastikan lisensi semuanya terkini dan terbaru, dan untuk memastikan standar industri masih dipatuhi. Audit perangkat lunak juga membantu mengungkap alat yang tidak digunakan dengan lisensi saat ini.

Menghapus perangkat lunak berlisensi yang tidak digunakan dapat membantu menghemat uang organisasi. Jika organisasi mengalami kurangnya visibilitas atau kendala dalam proses perangkat lunak, maka audit perangkat lunak bertindak sebagai pemeriksaan kesehatan untuk perangkat lunak yang sedang diaudit.

6.4 Jenis audit perangkat lunak

Tentu saja, mungkin ada lebih banyak bentuk audit perangkat lunak semua tergantung pada apa yang ingin dicapai dan apa kebutuhan Anda. Tetapi bentuk-bentuk ini adalah yang paling umum dan serbaguna. Mari kita lihat lebih dekat pada mereka:

1. Audit keamanan perangkat lunak
   Keamanan siber adalah masalah utama untuk setiap perusahaan yang matang. Serangan berbahaya dan pelanggaran keamanan dapat menyebabkan masalah serius, termasuk mengungkapkan informasi rahasia dan data pribadi karyawan, klien, dan mitra bisnis. Dalam skenario terburuk, pelanggaran semacam itu dapat menyebabkan akhir dari perusahaan. Itulah mengapa perusahaan di seluruh dunia melakukan apa pun yang mereka bisa untuk melindungi aset digital mereka. Mereka berinvestasi dalam firewall, perangkat lunak antivirus terbaik, transmisi data terenkripsi (SSL) dan bentuk hambatan digital lainnya.

Audit keamanan perangkat lunak adalah tentang memastikan bahwa semua perangkat lunak di perusahaan dilindungi dengan benar dan aman digunakan.

Selama audit keamanan perangkat lunak yang harus diperiksa:

- Apakah situs web perusahaan memiliki semua tindakan pencegahan yang diperlukan.
- Apakah perusahaan mematuhi peraturan keamanan data tertentu (misalnya, GDPR).
- Apa yang terjadi dengan data di perusahaan (bagaimana cara memprosesnya dan siapa yang memiliki akses ke sana)

2. Audit Ux (audit kegunaan dan aksesibilitas)

   Misalkan Anda mengembangkan perangkat lunak sendiri, katakanlah aplikasi seluler. Anda pasti ingin memastikan bahwa aplikasi tersebut dapat bekerja dan mudah digunakan, Hal ini yang dimaksud dengan audit UX. Selama audit semacam ini, auditor memeriksa alur pengguna dan pelanggan. Pada audit ini perlu dibuat panduan kognitif untuk memastikan aplikasi melakukan tugas yang berbeda secara akurat.

   Audit UX sangat penting untuk dilakukan sebelum mempublikasikan aplikasi baru. Pengecekan kemudahan sangat diperlukan, misalnya, calon pengguna dapat menganggap beberapa fitur sulit dipahami atau tidak dapat dipahami. Mengetahui bahwa Anda dapat melakukan modifikasi yang diperlukan dan menerbitkan produk yang 100% bermanfaat dan ramah pengguna. Itulah yang dimaksud dengan audit UX.

3. Audit kualitas perangkat lunak
   Jenis audit ketiga didasarkan pada verifikasi kualitas perangkat lunak Anda. Di sini, auditor memeriksa apakah semua aplikasi dan program yang digunakan diperbarui dan berfungsi dengan benar. Auditor juga perlu memeriksa apakah ada solusi lain yang dapat menggantikan alat saat ini dengan sesuatu yang lebih murah atau lebih efektif. Meskipun ini bukan poin utama, audit kualitas perangkat lunak juga dapat memverifikasi apakah menggunakan perangkat lunak legal dan tetap berpegang pada lisensi pengguna.
   Ingatlah bahwa saat ini, perangkat lunak berkembang pesat. Aplikasi berubah dan meningkat, dan jika tidak mengikutinya, maka secara sukarela perusahaan membuang waktu dan uang. Berkat audit kualitas perangkat lunak, Anda dapat yakin bahwa perusahaan Anda bekerja pada perangkat lunak yang efektif dan diperbarui.

6.5 Cara melakukan audit perangkat lunak

Biasanya, proses audit perangkat lunak terdiri dari empat tahap penting:

Tahap 1: Menentukan ruang lingkup dan tujuan audit

Audit harus terorganisir dengan baik. Anda perlu tahu apa yang harus diperiksa, bagaimana dan mengapa. Tidak ada ruang untuk tindakan yang tidak perlu – fokus hanya pada elemen yang benar-benar dapat memengaruhi cara kerja perusahaan.

Biasanya, lebih baik berkonsentrasi pada satu area tertentu dan pindah ke area berikutnya setelah selesai. Dengan cara ini, Anda tidak akan kewalahan dengan jumlah informasi yang Anda dapatkan. Pada titik ini, Anda harus berpikir tentang membuat daftar periksa audit perangkat lunak, menetapkan

pedoman transparan dan, tentu saja, memberi tahu tim tentang rencana audit.

Tahap 2: Memilih alat audit perangkat lunak

Di sini, kita memerlukan apa yang disebut alat SAM(Software Asset Management) yang merupakan praktik bisnis yang melibatkan pengelolaan dan pengoptimalan pembelian, penyebaran, pemeliharaan, pemanfaatan, dan pembuangan aplikasi perangkat lunak dalam suatu organisasi. Menurut ITIL, SAM didefinisikan sebagai "semua infrastruktur dan proses yang diperlukan untuk manajemen, kontrol, dan perlindungan aset perangkat lunak yang efektif" di semua tahap siklus hidup(Wikipedia, 2010).

Dengan alat SAM yang dipilih dengan benar, Anda akan bisa mendapatkan semua informasi yang Anda butuhkan dan melakukannya dengan cara yang efisien. Alat SAM yang tepat akan menyoroti kekurangan lisensi di perusahaan Anda, menunjukkan pengeluaran berlebihan, dan mendeteksi yang tidak digunakan yang dapat dihapus. Dengan kata lain, alat SAM pada dasarnya adalah layanan pihak ketiga objektif Anda yang akan memperkirakan data Anda dan memberi Anda laporan yang akurat.

Tahap 3: Melakukan audit

Beberapa alat SAM memungkinkan pengguna untuk menjalankan audit otomatis, tetapi Anda harus lebih banyak melakukannya secara manual daripada tidak, dan hal ini membutuhkan pengetahuan dan keahlian. Jika Anda belum pernah melakukan audit, kemungkinan besar, akan lebih baik untuk meminta bantuan seseorang. Bergantung pada jenis audit perangkat lunak yang ingin dilakukan.

Tahap 4: Analisis hasilnya

Seperti yang telah disebutkan sebelumnya, setiap audit harus memiliki tujuan. Temuannya harus digunakan untuk meningkatkan sesuatu di perusahaan Anda. Analisis hasil yang

didapatkan dan pikirkan tentang bagaimana pengetahuan ini dapat digunakan. Selanjutkan perlu menghubungkan data yang diterima pada tahap tiga ke tujuan awal yang Anda tetapkan pada tahap pertama.

6.6 Pedoman Pelaksanaan Audit Perangkat Lunak

1. Pahami lingkungan Anda dan datanya.
    a) Tinjau pengaturan ConfigMgr Anda:
        i. Apakah jadwal inventaris perangkat keras Anda diatur ke harian, mingguan, atau bulanan?
        ii. Apa pengaturan data lama Anda yang dihapus?
        iii. Apakah komputer dihapus dari AD saat dinonaktifkan?
    b) Apakah semua komputer (termasuk server) berada dalam ConfigMgr?
        i. Bagaimana dengan komputer di dalam DMZ?
    c) Bagaimana Anda mengelola komputer jarak jauh?
        i. Notebook/laptop?
        ii. Rata-rata seberapa sering komputer ini masuk ke jaringan? Atau mengembalikan inventaris ke ConfigMgr?
    d) Apakah Anda secara proaktif menyelesaikan masalah kesehatan klien?
2. Apakah Anda memiliki rencana siklus hidup komputer?
    a. Seberapa sering komputer diganti?
    b. Bagaimana Anda menentukan perangkat lunak apa yang harus dimigrasikan dari satu komputer ke komputer lain?
    c. Apa yang terjadi ketika seseorang memindahkan pekerjaan? Apakah daftar perangkat lunak di komputer mereka ditinjau untuk melihat apakah ada yang harus dihapus atau ditambahkan? Apakah

komputer dibawa bersama mereka atau tetap berada di kantor?

d. Apakah komputer direset ulang ketika pengguna lain menggunakannya?

3. Manajemen siklus hidup perangkat lunak.
   a. Apakah Anda menggunakan perangkat lunak versi lama?
   b. Kebijakan apa yang diberlakukan untuk meningkatkan versi perangkat lunak yang lebih lama?
   c. Siapa yang membayar untuk memutakhirkan perangkat lunak lama?
4. Kebijakan.
   a) Apakah Anda mengaudit siapa Administrator di setiap komputer?
   b) Apakah Anda meninjau proses pengadaan perangkat lunak setiap tahun?
   c) Apakah Anda meninjau bagaimana perangkat lunak diinstal pada setiap komputer? Apakah itu otomatis (ConfigMgr), apakah itu dilakukan oleh teknisi, atau keduanya?
   d) Bagaimana pengecualian untuk proses pengadaan perangkat lunak ditangani?
   e) Kapan manajemen terakhir meninjau dan menyetujui kebijakan pengadaan perangkat lunak?
   f) Bagaimana lisensi perangkat lunak dikendalikan?
   g) Apakah lisensi perangkat lunak ditinjau untuk memastikan keakuratan?
   h) Apakah perangkat lunak dihapus saat tidak lagi digunakan?
5. Data pelaporan.
   Cetak dan tinjau, "*Count of Add/Remove Programs* (ARP)." Dalam sistem operasi yang lebih baru, ARP juga dikenal sebagai, "Program dan Fitur," namun, di backend masih

akan dilihat sebagai ARP. Untuk lebih memperumit keadaan, dalam ConfigMgr, ARP sekarang disebut, "Aplikasi yang Diinstal."
Buat daftar judul perangkat lunak yang ingin Anda audit berdasarkan, "*Count of Add/Remove Programs*."

6. Audit perangkat lunak.
   a) Komputer apa yang memiliki jumlah ARP maksimum?
   b) Komputer apa yang memiliki jumlah minimum ARPs?
   c) Berdasarkan jumlah situs dan ukuran situs tersebut, pilih secara acak sampel komputer yang signifikan secara statistik. Cetak dan bandingkan ARPs di komputer itu sendiri dengan data ConfigMgr. Sekitar 100 komputer sudah cukup. Jika Anda tidak dapat membandingkan ARPs dengan data ConfigMgr untuk salah satu dari 100 komputer yang dipilih secara acak, jelaskan mengapa tidak.
   d) Buat laporan yang menunjukkan tanggal inventaris perangkat keras terakhir.
   e) Simpulkan seberapa andal data tersebut dalam laporan di atas.
7. Menguji keandalan data.
   a) Dari 100 komputer sampel, pilih 30 komputer tersebut secara acak dan lakukan audit penuh. Bandingkan data fisik tentang komputer tersebut: CPU, RAM, dan ukuran hard drive.
   b) Jika data tidak cocok, mengapa tidak? Apakah ini masalah kesalahan yang terisolasi, waktu, atau konsisten dalam populasi data yang lebih besar?
   c) Jika kesalahan dinilai didasarkan pada waktu atau masalah yang terisolasi, apakah Anda perlu menambah jumlah komputer yang perlu diuji?

8. Perhitungan.
    a) Bandingkan jumlah komputer di AD dengan ConfigMgr.
    b) Bandingkan jumlah komputer di ConfigMgr dengan data konsol AV.
    c) Berapa jumlah komputer yang dapat diterima yang hilang dari konsol AD/AV?
    d) Tentukan kapan perangkat lunak terakhir dijalankan dengan menggunakan tanggal aplikasi terbaru.
9. Siapkan laporan dan rekomendasi.
    a) Risiko apa yang ada?
    b) Perbaikan apa yang dapat dilakukan?
    c) Area apa yang terkendali?
    d) Bagaimana layanan pengguna akhir dapat ditingkatkan? Atau, jawab pertanyaan, "Mengapa pengguna akhir by-pass IT dan menginstal perangkat lunak sendiri?"
10. Jadwalkan audit perangkat lunak tindak lanjut.
    a) Tidak ada gunanya melakukan audit satu kali; Anda perlu membandingkan audit perangkat lunak dari waktu ke waktu untuk menentukan apakah Anda menjadi lebih baik. Jangka waktu enam hingga 12 bulan bagus.
    b) Jadwalkan tinjauan tahunan dari semua kebijakan yang relevan.
11. Mempresentasikan temuan kepada manajemen.(Jones, 2017)

6.7 Daftar periksa audit perangkat lunak

Memiliki daftar periksa audit perangkat lunak tentang langkah-langkah yang harus dilakukan sebelum audit dapat membantu proses mengalir lebih lancar. Daftar ini harus mencakup yang berikut:

- **Identifikasi ahli untuk audit.** Memilih kandidat untuk tim untuk menangani audit jika dan ketika mereka muncul adalah ide yang baik untuk dimiliki sebelumnya. Kandidat ini dapat berasal dari internal atau eksternal dan harus dapat menggunakan pengalaman mereka untuk menciptakan proses audit yang lancar.(Kolodiy, 2021)
- **Bersiaplah untuk proses audit.** Daftar ini harus mencakup kebijakan dan dokumentasi prosedur apa yang ada; perangkat keras, perangkat lunak, dan lisensi yang digunakan organisasi; dan bukti kepemilikan.

  Di sini pemangku kepentingan Anda harus menetapkan mengapa perangkat lunak harus diaudit. Anda perlu menunjukkan dengan tepat alasan audit proyek khusus ini dan bagaimana hal itu akan mendukung tujuan bisnis Anda. Selain itu, deteksi potensi risiko yang mungkin ditimbulkan oleh proyek ini dan cara menguranginya. Akhirnya, jika perangkat lunak telah diaudit sebelumnya, Anda perlu mengingatkan semua orang tentang hasil sebelumnya.

  Minta informasi yang akan membantu Anda memahami seluruh proses audit. Kumpulkan kebijakan, dokumentasi prosedur, dan laporan utama. Tanyakan tentang aplikasi yang digunakan untuk melakukan pemeriksaan dan daftar data yang diperlukan untuk itu. Dengan menggunakan data master, Anda akan memahami bagaimana prosesnya bekerja dan seperti apa hasilnya.
- **Siapkan Program Audit**

  Program audit adalah daftar langkah-langkah proses yang akan Anda ambil selama iterasi audit. Anda harus menentukan tujuan dan risiko proses serta cara untuk memitigasi risiko tersebut.
- **Lakukan tinjauan audit.** Tim manajer senior dan spesialis eksternal harus meninjau hasil audit perangkat lunak untuk menentukan langkah selanjutnya.

- **Gunakan alat manajemen aset perangkat lunak.** Alat SAM menganggarkan perangkat lunak, memungkinkan organisasi untuk lebih mudah menemukan dan memperbaiki kekurangan lisensi dan mendeteksi lisensi yang lebih lama dan tidak digunakan.

Apa yang harus dilakukan	Apa yang tidak boleh dilakukan
Segera teruskan surat audit kepada tim audit.	Yang terpenting, jangan melakukan apa pun yang dapat memiliki dampak hukum atau memberi kesan Anda telah mencoba memanipulasi hasil audit.
Konfirmasi dengan jelas penerimaan permintaan audit kepada auditor.	Jangan hapus contoh perangkat lunak yang dimaksud dari banyak mesin yang Anda yakini mungkin tidak sesuai. Jika audit diselesaikan di pengadilan, bahkan kemiripan ketidakwajaran bisa mahal.
Tambahkan klasifikasi "Pribadi dan Rahasia" ke semua komunikasi tentang audit.	Jangan berikan vendor akses langsung ke data.
Tentukan dewan audit RACI.	Jangan membagikan data apa pun dengan vendor audit tanpa izin dewan audit.
Minta semua pihak untuk menandatangani NDA.	Jangan menjalankan skrip apa pun untuk audit tanpa izin dari dewan audit.
Pastikan Anda memahami	

Apa yang harus dilakukan	Apa yang tidak boleh dilakukan
data sebelum mengirim ke auditor.	
Hanya berikan data yang diperlukan kepada auditor dan pastikan bahwa dewan audit Anda puas dengan data tersebut.	

6.8 Setelah audit perangkat lunak

Setelah auditor melakukan audit dan perekam mencatat item tindakan dan rekomendasi, auditor menjadwalkan pertemuan tinjauan audit perangkat lunak dengan organisasi yang sedang diaudit. Pertemuan ini membahas temuan laporan audit dan membahas potensi masalah. Auditor memberikan temuan mereka kepada organisasi sehingga dapat melakukan perbaikan pada bidang-bidang tersebut.

Sekali lagi, itu semua tergantung pada tujuan dan bentuk audit, tetapi biasanya, perusahaan setelah audit mereka memutuskan untuk:

- Hapus perangkat lunak yang tidak digunakan
- Perbaiki semua masalah teknis dan gangguan
- Atasi kemungkinan kebocoran keamanan
- Perbarui aplikasi dan alat usang
- Beli/unduh program baru atau beli lisensi baru
- Membuat laporan yang dapat meringkas proses audit
- Tetapkan rencana dan untuk tujuan berikutnya

DAFTAR PUSTAKA

Gillis, A. S. 2022. *Software Audit*, *TechTarget.com*. Available at: https://www.techtarget.com/whatis/definition/software-audit (Accessed: 28 March 2023).

Jones, G. 2017. *How to Perform a Basic Software Audit*, *RecastSoftware.com*. Available at: https://www.recastsoftware.com/resources/how-to-perform-a-basic-software-audit-2/ (Accessed: 28 March 2023).

Kolodiy, R. 2021. *Introduction to Software Audit: Definition, Benefits, Checklist*, *Techmagic*. Available at: https://www.techmagic.co/blog/introduction-to-software-audit/ (Accessed: 28 March 2023).

Otero, A. R. 2019. *Information Technology Control and Audit*. 5th edn. United States of America: CRC Press.

Wikipedia. 2010. *Software asset management*, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Software_asset_management (Accessed: 28 March 2023).

BAB 7
AUDIT PADA MANAJEMEN PROYEK IT

Oleh Santo Fernandi Wijaya

7.1 Pendahuluan

Salah satu dampak dari paska pandemi covid-19 yang melanda di Indonesia adalah terjadi perubahan pola hidup secara signifikan dari normal menjadi normal baru dimana kebanyakan orang melakukan kegiatan sehari-hari sangat tergantung terhadap sistem yang berbasis teknologi, seperti untuk memenuhi kebutuhan hidup hampir semua dilakukan dengan bertransaksi secara online dengan bantuan sistem berbasis teknologi. Juga kebanyakan orang sangat ketergantungan tinggi terhadap perangkat teknologi untuk memperoleh berbagai informasi sesuai keinginan dan kebutuhan sehari-hari. Hampir semua keinginan dan kebutuhan dapat dikerjakan dalam gengaman gadget yang dimiliki. Hal ini juga terjadi pada hampir semua sektor industri dimana adanya perubahan cara bisnis secara konvensional telah berubah menjadi cara bisnis secara digital. Hal ini menjadi tantangan bagi perusahaan-perusahaan untuk memastikan penggunaan sistem berbasis teknologi yang digunakan dapat dipercaya sesuai standar industri, sehingga penggunaan sistem berbasis teknologi ini dapat meningkatkan cara kerja yang lebih efisien, efektif dan produktivitas, yang akhirnya dapat memberikan keuntungan secara maksimal bagi perusahaan. Namun sebaliknya bila terindikasi terjadi kekacauan terhadap sistem berbasis teknologi yang digunakan

dalam menggerakan kegiatan bisnis perusahaan, maka hal ini akan menyebabkan kerugian finansial secara signifikan dan juga dapat mempengaruhi reputasi perusahaan, yang akhirnya perusahaan dapat menutup usahanya. Untuk itu, sangatlah dibutuhkan Audit.

7.2 Apa itu Audit?

Kata audit dalam pengertian umum berasal dari kata kerja "Mengaudit" yang memiliki arti menginspeksi, memeriksa, menilai, meninjau, menganalisis. Audit dapat membantu kita untuk lebih memahami secara detil mengenai kondisi atau situasi apakah yang telah kita lakukan telah sesuai standar yang ditentukan? Atau apakah kondisi kita masih aman atau sebaliknya apakah kondisi kita telah menyimpang terhadap pelaksanaan prosedur yang telah ditentukan. Biasanya perusahaan melakukan pelaksanaan audit terkait dengan kondisi keuangan dan sejumlah asset suatu perusahaan yang memiliki nilai secara signifikan. Tak mengherankan bagi perusahaan tertentu terdapat fungsi Internal Audit yang berfokus untuk melakukan pengontrolan terkait keuangan dan asset perusahaan. Audit merupakan alat penting untuk mengontrol dan menghindari terjadinya penipuan dan praktik korupsi yang dapat merugikan perusahaan. Audit adalah perencanaan kegiatan untuk memastikan kepatuhan pelaksanaan kegiatan melalui investigasi, evaluasi bukti objektif, kepatuhan terhadap proses dan standar yang ditetapkan, atau dokumen yang berlaku dan diimplementasikan. Audit dapat membantu dalam mencegah kerugian biaya suatu pihak yang tidak berkepentingan. Audit dapat melibatkan peninjauan proyek untuk memastikan kinerja yang dicapai telah sesuai dengan rencana dan tertuang dalam kontrak yang telah disepakati para pihak. Audit juga merupakan alat penting untuk menjaga agar kegiatan tetap

terkendali dan sesuai dengan anggaran yang disetujui [Okereke *et al.* 2022].

7.3 Audit TI

Hampir seluruh kegiatan operasional bisnis perusahaan digerakkan oleh dukungan perangkat Teknologi. Pemanfaatan Teknologi dapat lebih mendukung sasaran strategi bisnis perusahaan [Mansur dan Sofalina., 2022]. Untuk itu, diperlukan Audit TI untuk mencegah terhadap kehilangan data yang disebabkan ketidakmampuan pengendalian sistem yang digunakan, seperti tidak melakukan backup data secara rutin, sehingga mengakibatkan operasional kegiatan perusahaan menjadi terganggu, dan pengambilan keputusan berdasarkan informasi yang tidak berkualitas, juga penyalahgunaan akses tidak sesuai oleh orang yang tidak memiliki akses [Sihotang *et al.,* 2023]. Disamping itu, perlu memperhatikan faktor-faktor kritis dalam Audit TI untuk menentukan tingkat keberhasilan mengelola manajemen proyek. Faktor-faktor kritis yang perlu diperhatikan dalam manajemen proyek TI adalah sebagai berikut:

- Organisasi. Keberadaan organisasi untuk memastikan ketersediaan manajemen organisasi untuk melakukan proses *change management* dari tingkatan manajerial yang memiliki komitmen dalam menjalankan manajemen proyek. Proses *change management* ini dapat lebih menciptakan proses bisnis yang lebih transparan dan mendukung cara kerja dengan menggunakan sistem berbasis teknologi.
- Proses bisnis. Keberadaan proses bisnis untuk memastikan perubahan proses bisnis dengan menyesuaikan proses bisnis proyek TI yang sedang dijalankan, sehingga dapat lebih meningkatkan proses bisnis yang lebih *agile.*
- Infrastruktur TI. Keberadaan infrastruktur TI untuk memastikan ketersediaan infrastruktur TI yang memadai

dalam mendukung pelaksanaan proyek TI secara keseluruhan.
- Sistem aplikasi yang digunakan. Sistem aplikasi yang digunakan untuk memastikan integrasi dari sistem aplikasi yang digunakan dengan proses bisnis.
- Sumber Daya Manusia. Sumber Daya Manusia ini untuk memastikan ketersediaan pelatihan SDM terhadap penggunaan sistem berbasis Teknologi, sehingga para SDM dapat lebih memahami cara menjalankan Audit TI lebih transparan.

Berdasarkan hasil terhadap pengelolaan manajemen proyek TI, maka dibutuhkan tahapan evaluasi sebagai penilaian. Penilaian terhadap manajemen proyek TI merupakan hal penting yang harus dilakukan untuk mengetahui tingkat pencapaian dari target yang telah ditentukan sebelumnya [Mansur dan Sofalina., 2022]. Hasil penilaian evaluasi tersebut, diharapkan mampu memberikan rekomendasi solusi yang diusulkan terhadap permasalahan yang dihadapi perusahaan. Untuk itu, sangat penting dibutuhkan pelaksanaan Audit TI. Audit TI dapat berperan penting dalam mengevaluasi terhadap keefektifan kontrol keamanan perusahaan, dan merekomendasi perbaikan terhadap ketidakefektifan yang terjadi. Audit TI merupakan proses evaluasi terhadap sistem berbasis teknologi yang digunakan perusahaan yang bertujuan untuk memastikan sistem berbasis teknolori yang digunakan dalam keadaan aman, efisien, dan sesuai regulasi dan peraturan yang telah ditentukan. Oleh karena itu, Audit TI diperlukan untuk memastikan bahwa sistem berbasis teknologi dapat diandalkan dan aman dari serangan cyber. Audit IT juga bertujuan untuk memastikan penggunaan sistem berbasis teknologi dapat

berjalan sesuai *Standar Operating Prosedure*. Adapun kegiatan Audit TI meliputi sebagai berikut: [Sihotang et al., 2023].

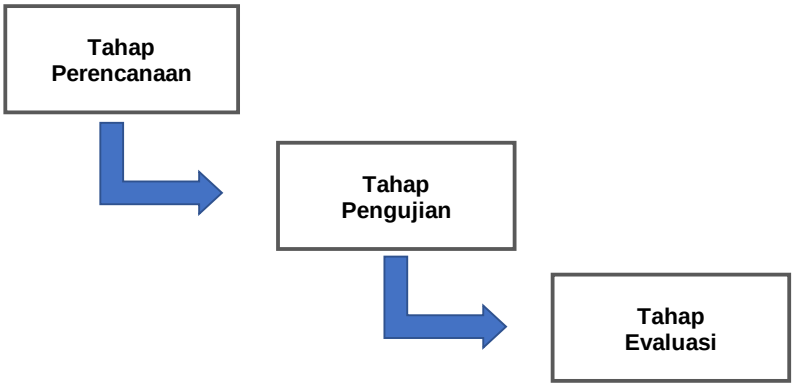
1. Audit terhadap penggunaan sistem berbasis teknologi. Hal ini untuk melakukan verifikasi cara kerja dan kontrol terhadap aplikasi telah memadai untuk memastikan input, proses, dan output telah dilakukan dengan valid, andal, tepat waktu, dan aman sesuai otorisasi dari pengguna yang menggunakan system aplikasi berbasis teknologi.
2. Audit terhadap fasilitas proses transaksi. Hal ini untuk memastikan proses transaksi telah dilakukan dengan tepat waktu, akurat, dan efisien.
3. Audit terhadap pengembangan sistem berbasis teknologi. Hal ini untuk memastikan sistem berbasis teknologi telah dikembangkan sesuai dengan standar yang berlaku secara umum.
4. Audit terhadap arsitektur TI. Hal ini untuk memverifikasi arsitektur TI telah mengembangkan sesuai prosedur yang efisien untuk pemrosesan berbagai informasi yang berkualitas untuk mendukung pengambilan keputusan bagi manajemen perusahaan.
5. Audit terhadap Server, Telekomunikasi, Internet. Hal ini untuk memverifikasi dan memastikan fungsi Server, Telekomunikasi, Internet berjalan sesuai *Standar Operating Prosedure* yang telah ditentukan.

Tujuan Audit TI untuk memastikan fungsi setiap departemen dalam perusahaan yang menggunakan system berbasis teknologi telah berjalan sesuai prosedur yang telah distandarisasikan, dan bila terjadi penyimpangan untuk dapat diberikan rekomendasi solusi perbaikan lebih lanjut. Tahap perencanaan Audit TI lebih berfokus untuk mengkaji kebijakan, tugas dan tanggung jawab setiap fungsi departemen dalam perusahaan yang tercermin dalam struktur organisasi. Pada

tahapan perencanaan ini juga dapat mengkaji standar prosedur, pengujian pengendalian dari setiap fungsi departemen perusahaan.

7.4 Tahapan Audit TI

Pada tahapan pengujian Audit TI lebih berfokus untuk melakukan pengujian pengendalian sesuai otorisasi setiap fungsi manajerial tiap departemen dalam perusahaan. Pada tahapan evaluasi Audit TI lebih berfokus untuk melakukan pengujian subtantif dengan membandingkan berbagai informasi-informasi yang disajikan dalam setiap sistem aplikasi berbasis teknologi yang digunakan, juga melakukan pengujian terhadap integrasi keterkaitan setiap transaksi terlebih bagi perusahaan yang menggunakan system aplikasi berbasis teknologi yang berbeda dalam menghasilkan berbagai laporan-laporan bagi manajemen perusahaan untuk pengambilan keputusan, termasuk laporan keuangan yang diberikan pihak ketiga, seperti auditor, perbankan dan perpajakan. Hal ini tentu akan mengambil kesulitan untuk melakukan konsolidasi dalam pelaporan. Jadi keterkaitan proses Audit TI mulai dari tahap perencanaan, pengujian, dan evaluasi dengan memiliki penekanan pada fungsinya. Penjelasan proses Audit TI tersebut dapat digambarkan pada gambar berikut:



Gambar 7.1. Tahapan Audit TI

7.5 Mengapa Audit Manajemen Proyek TI penting?

Kegagalan perusahaan dalam menerapkan fungsi Audit TI terhadap manajemen proyek TI, maka dapat menyebabkan terjadi kesalahan atas pencapaian hasil kinerja proyek TI menjadi buruk. Audit terhadap manajemen proyek TI berfungsi untuk menilai dan mengendalikan suatu proyek TI. Orang yang melakukan Audit manajemen proyek TI harus dapat bekerja tanpa gangguan apapun atau tanpa intervensi dari pihak manapun, sehingga proses Audit manajemen proyek TI dapat berjalan secara jujur dan transparan. [Okereke et al. 2022]. Audit manajemen proyek TI merupakan tinjauan secara formal terhadap suatu proyek yang dimaksudkan untuk menilai sejauh mana standar manajemen proyek berjalan baik atau sesuai prosedur. Untuk itu, Audit manajemen proyek TI sangat penting untuk memastikan bahwa manajemen perusahaan dapat menyediakan sumber daya, memberikan arahan, dan pengawasan yang memadai terhadap proyek TI. Audit manajemen proyek TI juga diperlukan untuk menghindari resiko-resiko seperti : menghindari penggunaan TI yang tidak

tepat, kesalahan pengulangan secara konsisten pada sistem berbasis teknologi yang digunakan, sistem yang tidak sesuai dengan proses bisnis, menghindari kerusakan infrastruktur komunikasi, menghindari informasi yang tidak akurat, dan menghindari otorisasi akses dari penguna terhadap sistem berbasis teknologi yang digunakan. Untuk itu, dibutuhkan orang yang mampu menjalankan proyek TI dan dapat dipercaya untuk mengkoordinasikan dan menggerakan kegiatan pada setiap tahapan proyek untuk memastikan dapat berjalan sesuai target yang telah ditentukan. Untuk itu sangat dibutuhkan seorang sebagai Manajer Proyek.

7.6 Manajer Proyek

Manajer proyek adalah orang yang harus memiliki kompetensi dan berpengalaman dalam menjalankan proyek TI dengan menerapkan pengetahuan teoritis dan praktis dalam mengelola proyek [Qusef dan Ismail., 2016]. Manajer proyek berfungsi sebagai pemimpin dan komunikator yang dapat mengkomunikasikan mengembangkan proses interaksi yang berkualitas dan hubungan secara kolaboratif dalam anggota tim proyek. Komunikasi dapat digunakan untuk mengkomunikasikan arus informasi, melakukan praktik partisipatif yang terlibat aktif, sehingga dapat menciptakan dan mengembangkan ide ide yang dapat dijadikan sebagai solusi dalam mengatasi permasalahan pada manajemen risiko. Manajemen risiko merupakan fokus utama dari Audit manajemen proyek TI untuk mengungkap area yang berpotensi terhadap risiko ketidakpatuhan. Untuk itu, peran manajer proyek TI sangat penting dalam mengendalikan manajemen risiko dengan merencanakan proyek secara efisien dan memastikan pengerjaan berjalan secara tepat waktu dan sesuai anggaran yang telah ditentukan.

7.7 Manajemen Proyek Agile

Dalam mengelola manajemen proyek dikenal dengan istilah Manajemen Proyek Agile yang berfokus untuk mempercepat proses dalam pengembangan suatu proyek. Manajemen Proyek Agile merupakan memperbaharui metode pengembangan secara tradisional (*waterfall atau spiral*). Manajemen Proyek Agile berbeda dengan manajemen proyek tradisional (*waterfall atau spiral*). Dalam metode tradisional, tim proyek menetapkan suatu tujuan tertentu, membuat serangkaian langkah untuk bisa mencapai tujuan dan melakukan proses implementasi, dan setiap tahapan harus diselesaikan secara tuntas untuk dapat melanjutkan pada tahapan berikutnya. Sedangkan dengan metode Manajemen Proyek Agile, membagi proyek menjadi tujuan-tujuan kecil atau sprint, dan menggunakan penilaian untuk melakukan langkah-langkah untuk memecahkan setiap permasalahan dalam tiap tahapan proses, dan setiap tahapan proyek dapat dikerjakan secara bersamaan dan juga dinilai secara pada waktu yang sama

Beberapa keuntungan dalam Penerapan Manajemen Proyek Agile seperti: umpan balik yang diberikan untuk diperbaiki atau dikembangkan secara cepat dalam kurun waktu yang relatif singkat, juga lebih responsif terhadap permintaan pengembangan proyek secara langsung, sehingga pengerjaan menjadi lebih efisiensi dengan mengendalikan biaya dan hasil pengerjaan secara nyata. Manajemen Proyek Agile memiliki karakteristik yang lebih fleksibilitas dalam proses pengorganisasian sebuah proyek. Manajemen Proyek Agile merupakan sebuah proses memecah permasalahan dalam proyek menjadi langkah-langkah taknis yang dapat dikelola dengan penekanan pada daya tanggap serta kolaborasi pelanggan.

Dalam praktis bisnisnya, cara Manajemen Proyek Agile dapat digunakan untuk mempercepat proses yang lebih cepat. Dengan penerapan Manajemen Proyek Agile dapat memberikan manfaat dalam setiap proses produksi, bukan hanya pada proses akhir saja. Dengan demikian penerapan Manajemen Proyek Agile ini dapat diterapkan pada semua industri, terutama yang berhubungan langsung dengan pengembangan produk.

DAFTAR PUSTAKA

Mansur, A., dan Sofalina, F. D. J. 2022. *Audit Penerapan Teknologi Informasi dengan Framework Cobit 4.1.* J-SAKTI (Jurnal Sains Komputer dan Informatika), 6(2), 1146-1153. http://dx.doi.org/10.30645/j-sakti.v6i2.523.

Okereke, R. A., Muhammed, U., & Eze, E. C. 2022. *Construction audits an essential project control function.* ITEGAM-JETIA, 8(33), 26-32. https://doi.org/10.5935/jetia.v8i33. 793.

Ruao, T., Marinho, S., & Silva, S. 2022. *Internal Communication in contemporary organizations: digital challenge in a project management department.* In Navigating Digital Communication and Challenges for Organizations (pp. 1-19). IGI Global. https://doi.org/10.4018/978-1-7998-9790-3.ch001.

Sihotang, J. I., Arni, S., Darsin, D., Ashari, I. F., Siregar, M. N. H., Fadhillah, Y., dan Yuniwati, I. 2023. *Kontrol dan Audit TI*. Yayasan Kita Menulis. ISBN: 978-623-342-715-9

BAB 8
FRAMEWORK DAN STANDAR AUDIT

Oleh Suwito Pomalingo

8.1 Pendahuluan

Meningkatnya ketergantungan pada sistem informasi berdampak pada peningkatan kebutuhan tata kelola dan pengendalian yang efektif. Hal ini menyebabkan audit teknologi informasi (TI) menjadi sebuah elemen penting dalam rangka memastikan integritas, keandalan, dan keamanan sistem informasi (Hall, 2015). Untuk mencapai tujuan tersebut, diperlukan framework dan standar audit yang dapat diandalkan sebagai pedoman dalam pelaksanaan audit TI.

Sangat penting untuk menggunakan framework dan standar audit yang tepat dalam melaksanakan audit TI yang efektif dan efisien. Keberhasilan audit TI sangat bergantung pada pemilihan dan penerapan framework dan standar yang sesuai. Penggunaan framework dan standar audit yang tepat akan memberikan beberapa manfaat, meliputi (Davis, Schiller and Wheeler, 2011):

a. Meningkatkan kualitas audit dengan menyediakan pedoman yang konsisten dan sistematis.
b. Mengurangi risiko kesalahan dan ketidakakuratan dalam proses audit.
c. Meningkatkan kepercayaan dan kredibilitas hasil audit.
d. Memfasilitasi komunikasi yang lebih baik antara auditor dan pihak yang diaudit.

e. Membantu organisasi memenuhi persyaratan peraturan dan kepatuhan yang relevan.

Framework audit merupakan kerangka kerja konseptual yang menyediakan struktur, proses, dan prinsip-prinsip dasar untuk melaksanakan audit TI secara efisien dan efektif (Hall, 2015). Framework audit mencakup metodologi, teknik, dan alat yang digunakan oleh auditor TI dalam menjalankan tugas mereka. Standar audit, di sisi lain, adalah peraturan dan pedoman yang ditetapkan oleh organisasi profesional atau badan pengatur yang menjelaskan praktik terbaik dan persyaratan minimum untuk melaksanakan audit TI (Kegerreis *et al.*, 2011).

8.2 COBIT (Control Objectives for Information and Related Technologies)

8.2.1 COBIT

COBIT atau *Control Objectives for Information and Related Technologies* merupakan framework yang dikembangkan oleh ISACA (*Information Systems Audit and Control Association*). COBIT adalah sebuah framework yang digunakan untuk membantu organisasi dalam pengelolaan dan pengendalian teknologi informasi, terutama dalam mengatasi tantangan tata kelola TI dan dapat membantu organisasi mencapai tujuan bisnis mereka melalui penerapan praktik terbaik dan kontrol yang efektif (ISACA, 2012). COBIT menekankan pada integrasi teknologi informasi dengan strategi dan tujuan bisnis secara keseluruhan (Grembergen and Haes, 2015).

COBIT 5 merupakan versi terbaru dari framework ini yang diterbitkan pada tahun 2012, dengan menggabungkan prinsip-prinsip dan praktik terbaik dari COBIT 4.1, Val IT, dan

Risk IT serta mengintegrasikannya dengan standar dan panduan lainnya, seperti ITIL dan ISO/IEC 27001.

8.2.2 Prinsip COBIT

Prinsip utama COBIT 5 meliputi:

1) *Meeting Stakeholder Needs*: COBIT 5 menekankan pentingnya memenuhi kebutuhan *stakeholder* atau pemangku kepentingan dengan menciptakan nilai melalui pengelolaan TI yang efektif.
2) *Covering the Enterprise End-to-End*: COBIT 5 mencakup seluruh organisasi, tidak hanya fungsi TI saja, hal ini untuk memastikan integrasi yang lebih baik antara TI dan strategi bisnis.
3) *Applying a Single, Integrated Framework*: COBIT 5 menyediakan framework terpadu yang mencakup semua aspek pengelolaan TI, termasuk tata kelola, manajemen risiko, dan kepatuhan.
4) *Enabling a Holistic Approach*: COBIT 5 menggunakan pendekatan holistik dengan melibatkan semua komponen organisasi, termasuk teknologi, informasi, serta orang dan struktur dalam pengelolaan TI.
5) *Separating Governance from Management*: COBIT 5 membedakan antara tata kelola dan manajemen. Tata kelola berkaitan dengan evaluasi, pengarahan, dan pemantauan TI, sementara manajemen berfokus pada perencanaan, pembangunan, dan pengoperasian TI dalam konteks strategi dan kebijakan yang telah ditetapkan oleh tata kelola.

8.2.3 Komponen Utama COBIT

COBIT terdiri dari beberapa komponen utama, yaitu:

1) *Process*: COBIT mencakup 40 proses yang dikelompokkan dalam 5 domain utama yakni *Evaluate*, *Direct*, *Monitor* (EDM); *Align*, *Plan*, *Organize* (APO); *Build*, *Acquire*, *Implement* (BAI); *Deliver*, *Service*, *Support* (DSS); dan *Monitor*, *Evaluate*, *Assess* (MEA). Proses ini mencakup berbagai aspek pengelolaan TI, mulai dari perencanaan strategis hingga pemantauan kinerja.
2) *Control*: COBIT menyediakan kontrol objektif untuk setiap proses. Kontrol objektif ini membantu organisasi dalam mengidentifikasi dan mengelola risiko yang terkait dengan teknologi informasi dan mencapai tujuan bisnis.
3) *RACI Chart*: COBIT menggunakan *RACI* (*Responsible, Accountable, Consulted, and Informed*) chart untuk mendefinisikan peran dan tanggung jawab individu dan tim dalam setiap proses.
4) *Maturity Models*: COBIT menyediakan model kematangan untuk membantu organisasi menilai tingkat kematangan proses TI mereka dan mengidentifikasi area yang memerlukan perbaikan.
5) *Goal and Performance Metrics*: COBIT mencakup metrik kinerja dan tujuan untuk membantu organisasi mengukur efektivitas proses dan kontrol mereka serta mencapai tujuan bisnis.

Sebagai framework tata kelola TI yang komprehensif, COBIT cocok untuk berbagai jenis organisasi, mulai dari perusahaan besar, organisasi yang tunduk pada peraturan ketat, perusahaan dengan risiko keamanan tinggi, organisasi publik dan pemerintah, perusahaan yang sedang berkembang, perusahaan yang ingin meningkatkan tata kelola TI, hingga organisasi yang menjalani audit TI.

8.2.4 Penerapan COBIT dalam Organisasi

Menerapkan COBIT dalam organisasi melibatkan beberapa langkah penting. Berikut adalah cara menerapkan COBIT dalam organisasi (ISACA, 2019):

- Pahami dan tentukan tujuan bisnis.
- Pahami COBIT framework
- Identifikasi kebutuhan organisasi.
- Tentukan prioritas dan sasaran.
- Kembangkan rencana implementasi.
- Terapkan kontrol dan proses COBIT.
- Monitor dan ukur kinerja.
- Tinjau dan perbaiki secara berkelanjutan
- Komunikasikan hasil dan pencapaian.

Demikian langkah-langkah penerapan COBIT dalam organisasi. Penting untuk diingat bahwa penerapan COBIT adalah proses berkelanjutan yang memerlukan komitmen dan dukungan dari seluruh pemangku kepentingan.

8.3 ITIL (Information Technology Infrastructure Library)

8.3.1 Pengantar ITIL

ITIL atau Information Technology Infrastructure Library merupakan framework yang menyediakan seperangkat kerangka kerja untuk pengelolaan layanan TI (ITSM) yang berfokus pada penyelarasan layanan TI dengan kebutuhan bisnis (AXELOS, 2011). ITIL pertama kali dikembangkan pada 1980-an oleh Central Computer and Telecommunications Agency (CCTA). Sejak awal, ITIL telah mengalami beberapa revisi. ITIL v2 diperkenalkan pada akhir 1990-an, menambahkan fokus pada kualitas layanan dan siklus hidup layanan. ITIL v3 diluncurkan pada 2007, menyediakan struktur

yang lebih matang dan terintegrasi yang mencakup 26 proses dan fungsi. ITIL 4, versi terbaru, diterbitkan pada tahun 2019 dan mencakup prinsip-prinsip dari Agile, DevOps, dan Lean, menyediakan kerangka kerja yang lebih fleksibel untuk mengatasi tantangan bisnis modern (AXELOS, 2019).

ITIL yang berfokus pada penyelarasan layanan TI dengan kebutuhan bisnis, dapat meningkatkan efisiensi dan efektivitas operasional, pengurangan biaya, peningkatan kualitas layanan, dan kepuasan pelanggan. ITIL membantu organisasi mengidentifikasi dan mengelola risiko, memastikan kepatuhan terhadap standar industri, dan menciptakan lingkungan yang mendukung peningkatan berkelanjutan. Dengan menggunakan ITIL, perusahaan dapat meningkatkan komunikasi antar tim, mengoptimalkan penggunaan sumber daya, dan mencapai tujuan bisnis mereka dengan lebih baik.

8.3.2 Prinsip-prinsip ITIL

Prinsip ITIL merupakan intisari filosofi ITIL yang membantu organisasi membuat keputusan yang efektif dan menjaga fokus pada penciptaan nilai bagi pelanggan.

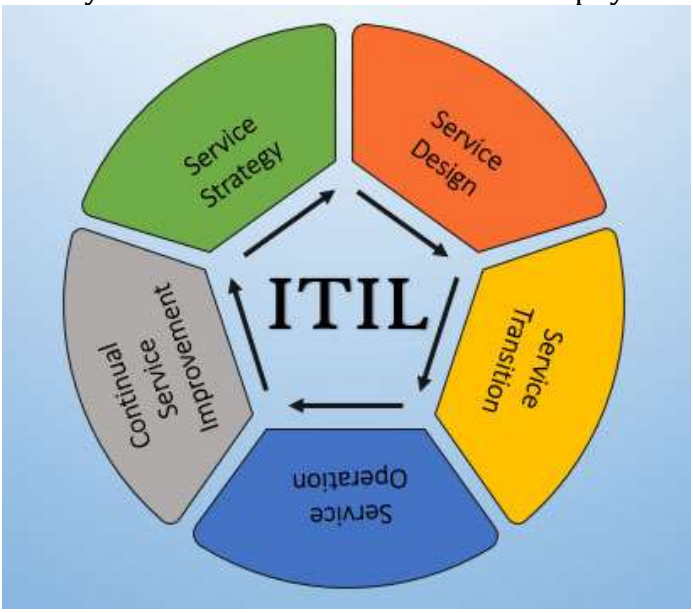
Terdapat tujuh prinsip panduan ITIL (AXELOS, 2019):

1) Fokus pada nilai, yakni memastikan layanan TI menciptakan nilai bagi pelanggan dan stakeholder.
2) Mulai dari tempat Anda berada, yakni bagaimana memanfaatkan aset, kemampuan, dan sumber daya yang ada saat merencanakan perubahan.
3) Berpikir dan bekerja secara holistik, yakni melihat gambaran besar dan mempertimbangkan bagaimana komponen sistem saling terhubung.
4) Progres iteratif dengan umpan balik, yakni mengadopsi pendekatan berulang yang memungkinkan penyesuaian berdasarkan umpan balik.

5) Bekerja secara kolaboratif, yakni melibatkan tim lintas fungsi dan menghargai kontribusi mereka.
6) Praktik transparansi, yakni menjaga komunikasi terbuka dan jujur dengan stakeholder.
7) Tetap sederhana dan praktis, yakni mengutamakan solusi yang sederhana dan mudah diimplementasikan.

8.3.3 Siklus Manajemen Layanan ITIL

Siklus layanan ITIL merupakan konsep utama dalam ITIL v3 yang menyediakan panduan tentang bagaimana mengelola layanan TI selama seluruh siklus hidupnya.



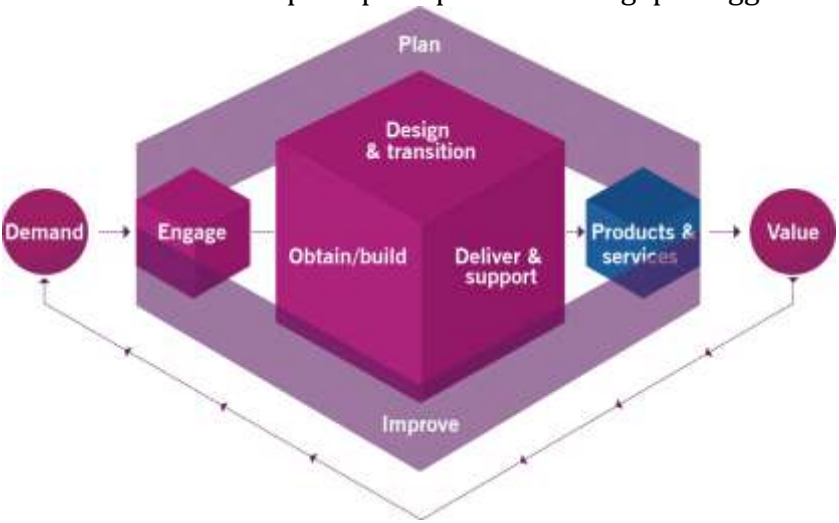
Gambar 8.1. ITIL Service Lifecycle
(Sumber : educba.com)

ITIL *Service Management* mempunyai sebuah siklus (*lifecycle*) yang terdiri dari 5 tahapan. Berikut penjelasan dari tahapan tersebut.

1) *Service Strategy* (Strategi Layanan) adalah inti dari siklus layanan ITIL. Berfokus pada pengembangan strategi layanan yang efektif untuk mendukung tujuan bisnis, dan mencakup identifikasi kebutuhan layanan, penetapan tujuan strategis, dan pengelolaan portofolio layanan.
2) *Service Design* (Desain Layanan) adalah adalah bagian produktif dari siklus layanan ITIL karena memberikan panduan bagi organisasi TI untuk dapat secara sistematis dan best practice mendesain layanan TI maupun implementasi ITSM itu sendiri. Tahap ini mencakup desain arsitektur layanan, kebijakan, dan proses yang diperlukan untuk mengelola layanan TI.
3) *Service Transition* (Transisi Layanan) menangani transisi layanan dari desain ke operasi, memastikan layanan baru atau yang ditingkatkan diimplementasikan dengan lancar dan efisien. Tahap ini mencakup perencanaan dan dukungan perubahan, manajemen rilis, dan pengelolaan risiko.
4) *Service Operation* (Operasi Layanan) berfokus pada pengelolaan operasi layanan TI sehari-hari, memastikan layanan dijalankan dengan efisien, efektif, dan sejalan dengan kebutuhan bisnis. Tahap ini mencakup pemantauan dan dukungan layanan, manajemen insiden, dan manajemen permintaan.
5) *Continual Service Improvement* (Peningkatan Layanan Berkelanjutan) mencakup pengidentifikasian dan implementasi perbaikan berkelanjutan dalam kualitas layanan TI, dengan tujuan untuk meningkatkan efisiensi, efektivitas, dan kepuasan pelanggan. Ini melibatkan pengukuran kinerja, analisis, dan rekomendasi perbaikan.

8.3.4 Service Value Chain ITIL 4

Service value chain atau model rantai nilai layanan dalam ITIL 4 merupakan evolusi dari siklus hidup layanan ITIL v3 dan menyajikan pendekatan yang lebih fleksibel dan terintegrasi untuk mengelola layanan TI dalam lingkungan bisnis yang dinamis. Model ini memungkinkan organisasi untuk lebih mudah beradaptasi dengan lingkungan bisnis yang dinamis dan berfokus pada penciptaan nilai bagi pelanggan.



Gambar 8.2. Service Value Chain ITIL 4
(Sumber : https://itsm.tools)

Service value chain ITIL 4 terdiri dari enam komponen utama:

1) *Plan*: Proses ini melibatkan penentuan strategi, kebijakan, dan portofolio layanan yang akan membantu organisasi mencapai tujuan bisnisnya. Mencakup pemahaman kebutuhan pelanggan, pengembangan visi dan misi layanan, serta alokasi sumber daya yang diperlukan.

2) *Improve*: Komponen ini mencakup identifikasi dan implementasi perbaikan yang berkelanjutan dalam kualitas, efisiensi, dan efektivitas layanan TI.
3) *Engage*: Aktivitas ini melibatkan interaksi dengan stakeholder, seperti pelanggan dan pengguna, untuk memahami kebutuhan mereka, mengkomunikasikan nilai layanan, dan mengumpulkan umpan balik yang akan membantu dalam pengembangan dan perbaikan layanan.
4) *Design & Transition*: Aktivitas ini melibatkan desain dan penilaian solusi layanan yang efisien dan efektif yang sesuai dengan strategi organisasi. Mencakup desain arsitektur layanan, kebijakan, dan proses yang diperlukan untuk mengelola layanan TI, serta transisi layanan dari desain ke operasi.
5) *Obtain* & *Build*: Aktivitas ini mencakup pengadaan, pengembangan, dan pembangunan komponen layanan TI yang diperlukan untuk mengimplementasikan solusi layanan yang telah didesain.
6) *Deliver* & *Support*: Aktivitas ini mencakup pengelolaan operasi layanan TI sehari-hari, termasuk dukungan, pemantauan, dan pemeliharaan layanan yang ada.

8.3.5 ITIL 4 *Practice*

ITIL 4 *practice* merujuk pada seperangkat panduan yang membantu organisasi mengelola layanan TI dan menciptakan nilai bagi pelanggan. *Practice* ini mencakup berbagai aspek manajemen layanan TI meliputi kegiatan teknis, operasional, serta strategis. ITIL 4 Practice dikelompokkan menjadi tiga kategori utama:

1) *General Management Practices*, mencakup prinsip dan teknik manajemen yang dapat diterapkan di berbagai bidang dan fungsi dalam organisasi. Beberapa contoh meliputi: manajemen portofolio layanan, manajemen

hubungan, manajemen kualitas, manajemen risiko, serta manajemen strategi.

2) *Service Management Practices*, spesifik untuk pengelolaan layanan TI dan berfokus pada aspek-aspek seperti desain, pengiriman, dan perbaikan layanan. Beberapa contoh meliputi: manajemen katalog layanan, manajemen perjanjian tingkat layanan, manajemen insiden, manajemen masalah, dan manajemen perubahan.
3) *Technical Management Practices*, melibatkan kegiatan teknis yang diperlukan untuk mendukung pengelolaan layanan TI, seperti pengelolaan infrastruktur, perangkat lunak, dan data. Beberapa contohnya meliputi manajemen kapasitas, manajemen kontinuitas layanan TI, manajemen keamanan informasi, manajemen konfigurasi, dan manajemen rilis.

8.3.6 Implementasi ITIL

Implementasi ITIL dalam organisasi melibatkan serangkaian langkah yang sistematis dan terstruktur. Berikut adalah langkah-langkah umum yang diperlukan untuk mengimplementasikan ITIL :

1) Pemahaman dan kesepakatan manajemen: memastikan bahwa manajemen puncak memahami manfaat ITIL dan mendukung implementasi. Tanpa dukungan manajemen, implementasi ITIL akan sulit dilakukan.
2) Penilaian situasi saat ini: melakukan penilaian terhadap praktik dan proses pengelolaan layanan TI yang ada untuk menentukan kekuatan dan kelemahan, serta mengidentifikasi area yang memerlukan perbaikan.
3) Penyusunan strategi implementasi: mengembangkan strategi implementasi yang mencakup tujuan, sasaran, jadwal, dan sumber daya yang diperlukan.

4) Pengembangan dan desain proses: menggunakan panduan ITIL untuk mengembangkan dan mendesain proses pengelolaan layanan TI yang baru atau ditingkatkan.
5) Pelatihan dan pengembangan kompetensi: melatih tim TI dan personel terkait mengenai konsep, prinsip, dan praktik ITIL untukmemastikan bahwa staf TI dan personel terkait memiliki pengetahuan dan keterampilan yang diperlukan untuk mengimplementasikan dan mengelola proses baru.
6) Implementasi dan transisi proses: meluncurkan proses yang telah didesain dan mengintegrasikannya ke dalam operasi sehari-hari. Ini mungkin melibatkan perubahan peran dan tanggung jawab, serta penggunaan alat dan teknologi baru.
7) Pengukuran dan perbaikan berkelanjutan: mengukur kinerja proses baru dan mengidentifikasi area yang memerlukan perbaikan. Proses perbaikan berkelanjutan akan memastikan bahwa pengelolaan layanan TI terus beradaptasi dan berkembang seiring waktu.

Contoh dalam melakukan implementasi ITIL dalam perusahaan sebagai berikut. Sebuah perusahaan jasa keuangan menghadapi masalah dalam manajemen insiden dan waktu pemulihan yang lama. Perusahaan ini memutuskan untuk mengimplementasikan ITIL untuk meningkatkan kualitas layanan TI yang diberikan kepada pelanggan dan karyawan. Langkah-langkah yang diambil perusahaan meliputi:

- Melakukan penilaian terhadap praktik pengelolaan insiden yang ada.
- Mendesain ulang proses pengelolaan insiden berdasarkan panduan ITIL.
- Melatih tim dukungan teknis dalam prinsip dan praktik pengelolaan insiden ITIL.

- Mengimplementasikan proses pengelolaan insiden yang baru dan sistem tiket dukungan.
- Melakukan pengukuran kinerja dan perbaikan berkelanjutan.

Setelah melakukan langkah tersebut, perusahaan berhasil mengurangi waktu pemulihan insiden dan meningkatkan kepuasan pelanggan dan karyawan. Implementasi ITIL membantu perusahaan mencapai efisiensi yang lebih baik dalam pengelolaan layanan TI dan memberikan nilai tambah yang signifikan bagi organisasi. Dengan pengalaman ini, perusahaan melanjutkan implementasi praktik ITIL lainnya, seperti manajemen masalah, manajemen perubahan, dan manajemen konfigurasi, untuk mencapai peningkatan yang lebih komprehensif dalam pengelolaan layanan TI mereka.

Penting untuk diingat bahwa dalam mengimplementasikan ITIL, setiap organisasi akan memiliki kebutuhan dan tantangan yang berbeda, sehingga pendekatan yang diambil mungkin akan berbeda. Namun, penjelasan diatas adalah langkah-langkah umum yang dapat membantu memastikan bahwa implementasi ITIL efektif dan berhasil dalam meningkatkan kualitas layanan TI dan menciptakan nilai bagi organisasi.

8.4 ISO/IEC 27001:2013 (Sistem Manajemen Keamanan Informasi)

8.4.1 ISO/IEC 27001 :2013

ISO/IEC 27001:2013 merupakan standar internasional yang menetapkan persyaratan untuk sistem manajemen keamanan informasi (*Information Security Management System/ISMS*). Tujuan utama dari ISMS adalah untuk melindungi aset informasi organisasi dari ancaman keamanan,

baik internal maupun eksternal, dengan mengidentifikasi risiko dan mengimplementasikan kontrol keamanan yang sesuai. Standar ini mencakup aspek teknis, administratif, dan fisik keamanan informasi dan membantu organisasi mengelola dan melindungi informasi yang penting, termasuk data pribadi, informasi keuangan, dan informasi bisnis yang rahasia (iso.org, 2013)

Implementasi ISO/IEC 27001:2013 melibatkan pengembangan, pemeliharaan, dan peningkatan berkelanjutan dari ISMS yang mencakup kebijakan, prosedur, dan kontrol keamanan yang sesuai. Standar ini juga mendorong pendekatan berbasis risiko, di mana organisasi secara proaktif mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan informasi, serta merencanakan dan mengimplementasikan kontrol yang efektif untuk mengurangi risiko tersebut. Selain itu, ISO/IEC 27001:2013 memungkinkan organisasi untuk mencapai sertifikasi ISMS oleh badan sertifikasi independen, yang dapat meningkatkan reputasi dan kepercayaan dari pelanggan, mitra, dan pemangku kepentingan lainnya.

8.4.1 Aspek Penting dalam ISO/IEC 27001 :2013

ISO/IEC 27001:2013 mencakup beberapa aspek penting saat mengimplementasikan sistem manajemen keamanan informasi (ISMS). Berikut adalah beberapa area kunci yang perlu diperhatikan (ISACA, 2017):

- Ruang Lingkup: Menetapkan batasan dan ruang lingkup ISMS, termasuk organisasi, lokasi, aset, dan teknologi yang relevan.
- Kebijakan Keamanan Informasi: Mengembangkan kebijakan keamanan informasi yang mencerminkan tujuan dan komitmen organisasi dalam melindungi aset informasinya.

- Penilaian Risiko: Melakukan penilaian risiko secara berkala untuk mengidentifikasi ancaman dan kerentanan terhadap aset informasi, serta mengevaluasi dampak potensial dari realisasi risiko tersebut.
- Perlakuan Risiko: Menyusun strategi perlakuan risiko yang mencakup penerapan kontrol keamanan yang sesuai, pemindahan risiko, penerimaan risiko, atau menghindari risiko.
- Pemilihan Kontrol: Memilih kontrol yang sesuai dari Annex A ISO/IEC 27001, yang mencakup 114 kontrol yang dikelompokkan ke dalam 14 kelompok, atau mengadopsi kontrol tambahan yang relevan dengan organisasi.
- Pernyataan Aplikabilitas: Mendokumentasikan kontrol yang dipilih dan memberikan penjelasan mengenai keputusan pemilihan, serta menjelaskan kontrol yang dianggap tidak relevan.
- Pengendalian Operasional: Mengelola dan memonitor kontrol keamanan yang telah diimplementasikan, serta memastikan bahwa kebijakan dan prosedur diikuti secara konsisten.
- Komunikasi dan Kesadaran: Menyediakan informasi dan pelatihan yang diperlukan untuk meningkatkan kesadaran dan pemahaman tentang kebijakan, prosedur, dan kontrol keamanan informasi di seluruh organisasi.
- Pengukuran Kinerja: Mengukur kinerja ISMS dan efektivitas kontrol keamanan menggunakan metrik yang relevan, serta melaporkan hasilnya kepada manajemen.
- Audit Internal dan Tinjauan Manajemen: Melakukan audit internal secara berkala untuk memastikan kepatuhan terhadap standar dan kebijakan keamanan informasi, serta melakukan tinjauan manajemen untuk mengevaluasi efektivitas ISMS secara keseluruhan.

- Perbaikan Berkelanjutan: Mengidentifikasi dan mengimplementasikan perbaikan yang diperlukan berdasarkan hasil audit, tinjauan manajemen, dan pengukuran kinerja, serta menanggapi insiden keamanan dan perubahan lingkungan.

Dengan membahas area-area penting ini dalam implementasi ISO/IEC 27001:2013, organisasi akan mampu mengelola risiko keamanan informasi secara efektif dan menciptakan lingkungan yang aman untuk melindungi aset informasi yang penting.

8.5 ISACA (*Information Systems Audit and Control Association*)

ISACA (*Information Systems Audit and Control Association*) adalah sebuah asosiasi profesional global yang didirikan pada tahun 1969 dan berfokus pada tata kelola teknologi informasi (TI), audit TI, kontrol, keamanan, dan manajemen risiko. ISACA menawarkan sertifikasi yang diakui secara internasional, seperti *Certified Information Systems Auditor* (CISA), *Certified Information Security Manager* (CISM), *Certified in the Governance of Enterprise IT* (CGEIT), dan *Certified in Risk and Information Systems Control* (CRISC). Selain itu, ISACA juga mengembangkan kerangka kerja dan panduan praktik terkemuka, seperti COBIT (*Control Objectives for Information and Related Technologies*), yang membantu organisasi dalam pengelolaan dan tata kelola TI yang efektif.

ISACA mempromosikan pertukaran pengetahuan dan praktik terbaik melalui jaringan lokal (chapter), konferensi, publikasi, dan webinar. Referensi terkait ISACA meliputi situs web resmi mereka (https://www.isaca.org/) dan berbagai publikasi yang diterbitkan oleh asosiasi tersebut, seperti COBIT

2019, ITAF (*Information Technology Assurance Framework*), dan banyak lagi.

8.6 NIST (*National Institute of Standards and Technology*)

NIST *Cybersecurity Framework* adalah *framework* yang dikeluarkan oleh NIST (*National Institute of Standards and Technology*) sebuah lembaga federal Amerika Serikat yang berada di bawah Departemen Perdagangan yang didirikan pada tahun 1901 dan berfokus pada kemajuan ilmu pengetahuan, teknologi, dan inovasi melalui pengembangan standar, pengukuran, dan praktik terbaik. Salah satu bidang fokus NIST adalah keamanan siber dan perlindungan informasi, yang mencakup pengembangan kerangka kerja, panduan, dan rekomendasi untuk membantu organisasi melindungi infrastruktur teknologi informasi dan sistem mereka.

NIST *Cybersecurity Framework* adalah salah satu hasil kerja NIST yang paling dikenal dan banyak digunakan di seluruh dunia. Kerangka kerja ini menyediakan panduan yang fleksibel dan dapat disesuaikan untuk membantu organisasi mengelola dan mengurangi risiko siber. NIST juga mengembangkan standar dan panduan keamanan informasi lainnya, seperti NIST SP 800-53 (*Security and Privacy Controls for Federal Information Systems and Organizations*) dan NIST SP 800-171 (*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*). Publikasi NIST ini membantu organisasi, baik pemerintah maupun swasta, dalam mengimplementasikan praktik keamanan yang efektif dan meningkatkan postur keamanan mereka.

DAFTAR PUSTAKA

AXELOS. 2011. *ITIL Service Strategy*. TSO (The Stationery Office).

AXELOS. 2019. *ITIL Foundation: ITIL 4 Edition*. TSO (The Stationery Office).

Davis, C., Schiller, M. and Wheeler, K. 2011. *IT Auditing Using Controls to Protect Information Assets*. 2nd Editio. New York, NY, USA: McGraw-Hill Education.

Grembergen, W. Van and Haes, S. De 2015. *Enterprise Governance of Information Technology Achieving Alignment and Value, Featuring COBIT 5*. Springer International Publishing.

Hall, J. A. 2015. *Information Technology Auditing*. 4th edn. Cengage Learning.

ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Available at: https://www.isaca.org/resources/cobit (Accessed: 13 March 2023).

ISACA. 2017. *Implementation Guideline ISO/IEC 27001:2013*.

ISACA. 2019. *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

iso.org. 2013. *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Available at: https://www.iso.org/standard/54534.html (Accessed: 15 March 2023).

Kegerreis, M. *et al.* 2011. *IT Auditing Using Controls To Protect Information Assets*. Third Edit. New York, NY, USA: McGraw-Hill Education.

BAB 9
MANAJEMEN RISIKO

Oleh Alfrian C Talakua

9.1 Pengenalan

Risiko pada umumnya merupakan keadaan kerugian atau kehilangan yang dapat terjadi karena kelalaian, kesalahan manusia ataupun mesin, hal ini disebabkan oleh kondisi lingkungan, ancaman, bencana alam yang terjadi pada suatu lingkungan. Bagi organisasi atau perusahaan risiko merupakan sebuah kemungkinan – kemungkinan yang akan terjadi yang dapat merugikan perusahaan atau organisasi. Pada hakikatnya risiko memiliki dampak yang negatif bagi sasaran dan strategi perusahaan yang ingin dicapai. Sehingga risiko dan akibatnya terhadap bisnis merupakan hal penting untuk yang perlu diidentifikasi dan diukur sejak awal. Menurut Paul Hopkins Risiko merupakan potensi bahaya yang ditimbulkan jika suatu ancaman dapat mengeksploitasi kelemahan tertentu, sehingga menyebabkan kerusakan pada aset-aset penting dalam sebuah organisasi. Paul Hopkins juga menjelaskan beberapa definisi terkait dengan risiko, berdasarkan *Oxford English Dictionary* risiko didefinisikan sebagai peluang atau kemungkinan bahaya, kehilangan, cedera atau konsekuensi buruk lainnya. *Institute of Risk Management* (IRM) mendefinisikan risiko sebagai kombinasi kemungkinan sebuah kejadian dan konsekuensinya.(Paul Hopkin, 2017) Dalam ISO Guide 73, risiko didefinisikan sebagai akibat dari ketidakjelasan tujuan. Dampak atau akibat serta konsekuensi yang muncul mungkin positif, negatif atau penyimpangan dari apa yang diharapkan. Dalam perkembangan dunia teknologi,

perusahaan atau organisasi yang menggunakan IT sebagai pendukung utama dalam proses bisnis harus dengan benar dan teliti dalam mengidentifikasi risiko yang akan terjadi kedepan, dikarenakan ketergantungan proses bisnis terhadap IT saat ini sangat tinggi, pemanfaatan IT juga memiliki risiko yang cukup besar. Perusahaan atau organisasi sering berinvenstasi besar pada bidang IT guna mendukung kinerja proses bisnis, namun pada kenyataannya sebagian besar mengalami kerugiaan jangka panjang karena pembiayaan *maintenance* yang tidak terduga. Hal ini terjadi karena perusahaan atau organisasi hanya berorientasi pada hasil yang diinginkan dalam waktu yang singkat, namun tidak merencanakan dengan baik untuk jangka panjang. Banyak risiko yang dapat terjadi selain proses *maintenance* yang buruk, pada akhirnya terjadi kerugian pada pembiayaan yang tak terduga, sehingga untuk meminimalisir hal tersebut diperlukan sebuah manajeman risiko. Manajemen risiko merupakan suatu proses yang dilakukan untuk mengidentifikasi, analisis, dan melakukan penilaian, pengendalian, dan upaya untuk menghindari, meminimalisir risiko pada perusahaan atau organisasi. Manajemen risiko perlu dilakukan oleh perusahaan atau organisasi untuk mengenali, mengidentifikasi, mengelola risiko serta kejadian yang mungkin akan muncul, untuk meminimalkan dampaknya dan menentukan penanganan risiko yang tepat guna meningkatkan peluang sukses. Proses analisis manajemen risiko merupakan kegiatan yang dilakukan pada tingkat pimpinan pelaksana dalam sebuah perusahaan atau organisasi, proses ini berupa kegiatan penemuan dan proses analisis sistematis atas kerugian yang mungkin saja dapat dihadapi oleh perusahaan atau organisasi, akibat suatu risiko serta cara pengendalian yang paling tepat untuk menangani kerugian yang dihubungkan dengan tingkat keuntungan perusahaan. Kadang perusahaan atau organisasi berpikir

bahwa risiko yang diidentifikasi merupakan hal yang tidak mungkin terjadi sehingga menjadi hal yang dikatergorikan dalam sebuah ketidakpastian untuk menekan pembiayaan dalam hal persiapan mitigasi risiko. Namun pemikiran seperti ini yang akan menjadi berbahaya jika risiko tersebut menjadi realita, sehingga kita perlu membedakan antar risiko dan ketidakpastian. Perusahaan atau organisasi yang baik harus menerapkan manajemen risiko sehingga tujuan utama dapat tercapai dengan baik dengan tingkat risiko yang diminimalisir.

9.2 Karakteristik Risiko

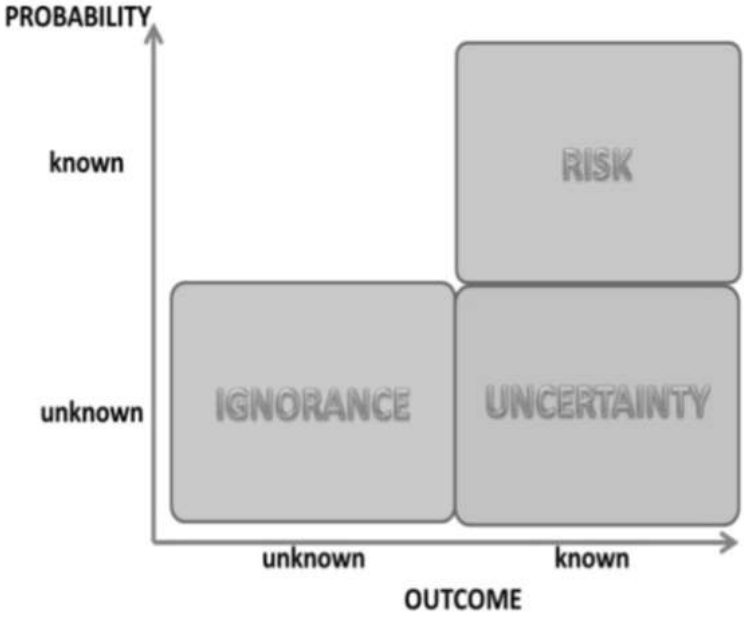
Karakteristik risiko dibagi menjadi 2 bagian yaitu ketidakpastian dan kerugian secara umum risiko sebenarnya merupakan bentuk dari ketidakpastian, akan tetapi ketidakpastian belum tentu mengandung risiko, oleh karena itu, perlu pemahaman sudut pandang antara risiko dan ketidakpastian sebelum melakukan pengembangan sebuah sistem informasi.(Hairul, 2020)

9.2.1 Ketidakpastian

Ketidakpastian atau *uncertainty* dapat dikatakan suatu keadaan didiman kemungkinan kejadian atau setiap kejadian akan menyebabkan hasil yang berbeda. Tetapi, probabilitas kejadian itu sendiri tidak diketahui secara kuantitatif. Ketidakpastian juga merupakan kejadian yang menandai risiko atau tidak mungkin terjadi.

Penjelasan terkait dengan posisi antara risiko dan ketidakpastian dengan ketidaktahuan terlihat pada Gambar.1 dimana risiko maupun ketidakpastian sama-sama memiliki dampak terhadap kemungkinan kejadian atau kerugian. Sementara ketidaktahuan belum bisa dipastikan.

"All Risks are ucertain, however not all uncertainties are risk"



Gambar 9.1. Risiko dan Ketidakpastian
(Sumber : Manajemen Risiko TI)

Untuk lebih memahami perbedaan antara risiko dan ketidakpastian, umumnya dalam sebuah proyek sistem informasi akan didahului dengan kajian risiko yang dikenal dengan RBS (*Risk Breakdown Structure*) (Risma, 2021)

Gambar 9.2. Risk Breakdown Structure
(Sumber : Manajemen Risiko TI)

Pada gambar 9.2 menjelasakan terkait membagi kategori dan sub kategori dalam sebuah organisasi atau sebuah project agar lebih mudah dalam mengidentifikasi risiko. Pada struktur yang dibangun untuk menidentifikasi risiko ada 3 elemen utama yang saling beririsan, yaitu *People, Process* dan *Technology* dari ketiga elemen inilah penyebab munculnya risiko. (ISO 38500, 2008)

9.2.2 Kerugian

Karakteritik yang berikut adalah kerugian, yang merupakan dampak dari kejadian yang teridentifikasi risiko menjadi realita. Hal ini dapat berdampak buruk bagi tujuan perusahaan atau organisasi jika nilai risiko yang teridentifikasi memiliki nilai yang tinggi.

9.3 Klasifikasi Risiko

9.3.1 Risiko Murni

Risiko yang hanya bisa dihadapi atau ditanggulangi dan tidak bisa dicegah, jika dikaitkan dengan penggunaan Teknologi Informasi maka risiko ini akan berdampak pada kerugian yang besar. Sehingga perusahaan dan organisasi menggunakan cara penanggulangan dengan mengasuransikan asset – asset penting. Contoh dari kerugian secara murni yang tidak bisa dicegah seperti bencana alam.

9.3.2 Risiko Spekulatif

Risiko ini akan terjadi jika ada pengambilan keputusan dari pimpinan perusahaan atau organisasi dengan mempertaruhkan kerugian sebagai satu sisi yang pasti, sehingga jika ada musibah, perusahaan atau organisasi rugi, namun jika tidak ada musibah, perusahaan untung. Contoh pada penggunaan teknologi informasi ialah jika suatu perusahaan mencoba untuk berinovasi pada bidang IT dengan berinvestasi besar untuk mengikuti *trand* namun secara internal dalam proses membangun 3 elemen penting. Hal ini bisa berdampak baik jika dapat digunakan dengan baik untuk menunjang proses bisnis kedepan namun juga dapat menjadi kerugian jika inovasi yang dilakukan tidak memberikan efek yang baik bagi kinerja proses bisnis sehingga akan mengalami kerugian terhadap investasi yang telah dilakukan.

9.3.3 Risiko Keuangan

Risiko keuangan bisa terjadi seperti risiko pasar, risiko likuiditas dan risiko kredit, jika dikaitkan dengan teknologi informasi bisa dicontohkan sebagai suatu organisasi yang memanfaatkan teknologi dengan pembiayaan yang dilakukan dengan sistem sewa bardasarkan jumlah object, hal ini tidak akan berdampak besar pada keuangan, jika jumlah object

masih tergolong sedikit, namun jika bisnis berkembang dan object bertambah banyak maka pengeluaran untuk penyewaan juga bertambah besar dan jika bisnis mengalami penurunan namun harus tetap membayar sewa aplikasi/sistem dengan jumlah object yang besar maka akan berakibat pada kerugian keuangan. Sehingga perlu dengan teliti dalam merencanakan keuangan dengan baik sebelum berinvestasi jangka Panjang menggunakan teknologi informasi.

9.3.4 Risiko Operasional

Risiko operasional ini bersifat internal hal ini dapat terjadi pada kegagalan proses bisnis dalam memproduksi produk, pelayanan yang buruk, keamanan data yang buruk karena maintenance kegagalan sistem, sehingga terjadi kerugian bagi perusahaan, risiko ini sering muncul dari kesalahan atau kegagalan sumber daya manusia pada organisasi atau perusahaan tersebut.

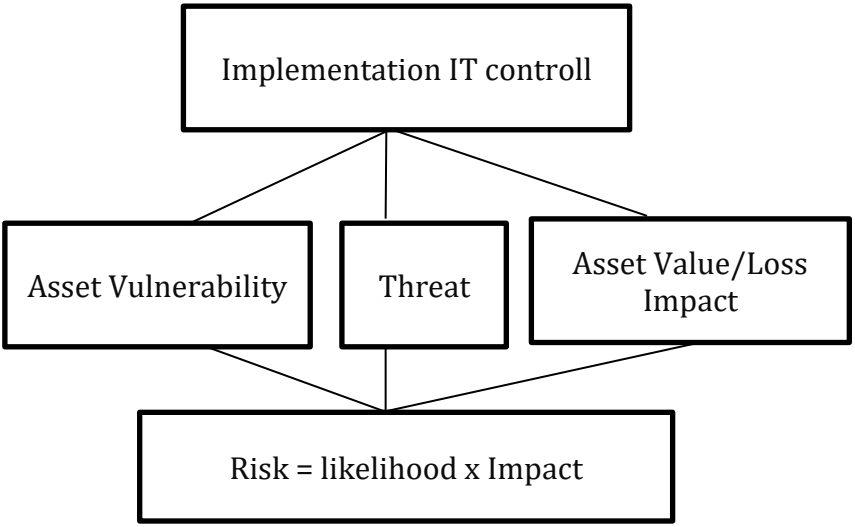
9.3.4 Risiko Strategis

Risiko ini sering berkaitan dengan setiap keputusan yang diambil oleh perusahaan atau organisasi karena gagal dalam mengantisipasi perubahan lingkungan bisnis, setiap keputusan yang diambil harus memikirkan resiko yang akan terjadi hal ini akan berdampak pada kompetisi atau persaingan, risiko inovasi teknologi, risiko kerusakan *image* dari merek dagang. Sehingga perlu menyusun strategi yang baik agar dapat bersaing dan tetap menjaga nilai jual yang baik di pasar.

9.3.5 Risiko Teknologi Informasi

Berikut merupakan risiko yang ditujukan pada perusahaan atau organisasi yang telah bergantung penuh dalam penggunaan teknologi informasi. Risiko TI terjadi karena ada kemungkinan -kemungkinan ancaman yang terjadi untuk

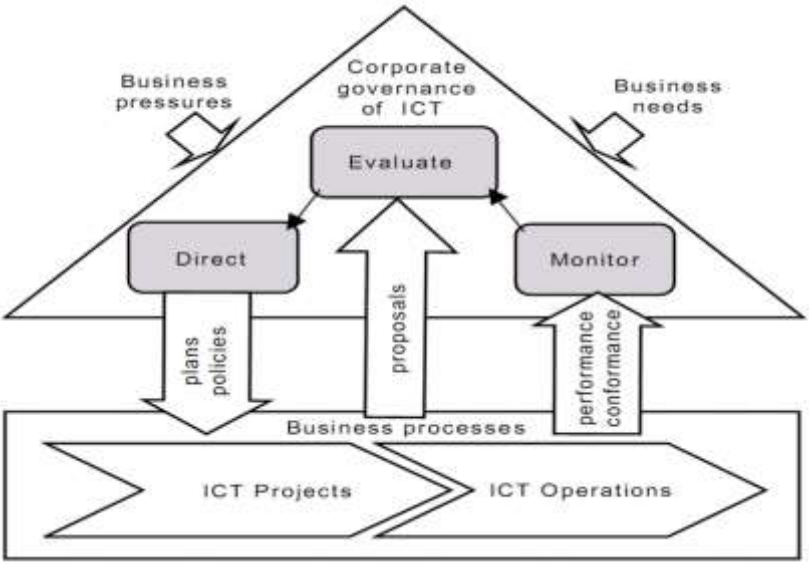
mengeksploitasi kerentanan pada sebuah asset dan menghasilkan dampak bisnis yang merugikan organisasi. Untuk meminimalisir risiko tekonologi informasi maka perlu untuk menerapkan *IT Controll* yang baik dengan memperhatikan perhitungan nilai resiko, banyak asset IT yang harus terkontrol dengan baik agar dapat menunjang proses bisnis. Dari segi asset fisik, asset software, hingga asset SDM semua perlu diperhatikan dengan baik. Pada umumnya nilai resiko dihitung berdasarkan kemungkinan per frekuensi dikali dengan *impact* atau dampak yang akan diterima, sehingga dengan perhitungan tersebut depat dikaitkan pada penerapan teknologi informasi untuk mendeteksi kemungkinan dan dampak yang dapat menghasilkan resiko dari asset TI yang dimiliki. Hubungan dari resiko dan *IT Controll* dapat terlihat pada gambar 9.3.



Gambar 9.3. *IT Controll and Risk*
(Sumber : Penulis)

Berdasarkan gambar diatas dijelaskan bahwa jika kemungkinan (*likelihood*) kecil dan dampaknya besar maka potensi resiko menjadi kecil, kemungkinan ditentukan dari kerentanan aset IT dan ancaman, aset dari TI bisa berupa aplikasi atau sistem, pengguna dan aset fisik lainya. Aset TI bisa saja memiliki kelemahan, hal inilah yang akan menjadi potensi ancaman. Sebaliknya jika aset TI dapat dikendalikan dengan baik maka ancaman juga dapat diminimalisir dan juga dapat menurunkan tingkat resiko. Selain itu aset juga memiliki *value* yang harus dijaga maupun ditingkatkan, seperti asset fisik TI yang memiliki tingkat *update* yang cukup singkat sehingga harus diperhatikan saat berinvestasi, perlu dianalisis nilai penggunan asset TI memiliki jangka waktu yang panjang, sehingga tidak menimbulkan kerugian pada keuangan organisasi atau perusahaan, hal yang sama berlaku juga pada aset TI yang lain.

Level Resiko IT



Gambar 9.4. *Model for corporate governance of ICT*
(Sumber : ISO38500 (2008))

Pada gambar 9.4. Berdasarkan level resiko TI dibagi menjadi 3 bagian berdasarkan *Model for corporate governance of ICT*. Level yang pertama ialah strategi perusahaan atau organisasi, pada level ini akan diidentifikasi resiko terkait kesesuaian penggunaan IT untuk menunjang proses bisnis sesuai dengan tujuan, yang kedua ialah level project TI pada level ini akan diidentifikasi resiko terkait ketepatan waktu dalam pengerjaan project, pembiayaan project dan hasil project. Pada level yang ketiga terjadi pada operational ketika perusahaan melakukan implementasi TI dalam masa pengoperasiannya cukup rentan terjadinya resiko TI.(ISO 38500, 2008)

Penyebab Risiko TI

a. Kelemahan Tata Kelola TI

Perusahaan kadang kurang menerapkan tata kelola TI dengan benar padahal memanfaatkan TI sebagai faktor utama untuk menunjang proses binis. Kelemahan ini mengakibatkan kesalahan dalam pengambilan keputusan terkait TI.

b. Kompleksitas Aset TI yang tidak terkendali

Semakin tinggi kebutuhan pada sistem atau aplikasi yang digunakan maka semakin tinggi tingkat kerumitan atau komplekstitas yang dibutuhkan untuk membangun sebuah sistem atau aplikasi, dengan tingkat kerumitan yang tinggi maka rentan dengan gangguan dan keamanan. Hal inilah yang menjadi sumber risiko TI bagi perusahaan atau organisasi. Ancaman dari sumber aset yang lain juga ialah pada *value* dari SDM yang dimiliki, yang berikutnya adalah ketergantungan pada pihak ketiga jika kita menggunakan pihak ketiga dalam membangun aplikasi atau sistem yang digunakan.

c. Tidak Peka terhadap Sumber Risiko

Ketidakpekaan terhadap risiko TI hal ini berkaitan juga dengan perancangan strategis seperti contoh perekrutan SDM, terkadang SDM yang direkrut tidak sesuai dengan kebutuhan perusahaan atau organisasi, atau kurang pelatihan untuk peningkatan skill bagi SDM sehingga SDM tidak berkembang.

9.4 Proses manajemen risiko

Proses manajemen resiko dilakukan untuk menekan tingkat risiko yang akan terjadi pada perusahaan, banyak *framework* dan standar yang digunakan untuk membantu perusahaan atau organisasi proses manajemen risiko TI. Berikut beberapa *framework* yang cukup sering digunakan oleh

perusahaan atau organisasi dalam menerapkan tata kelola TI dan juga untuk melakukan manajemen risiko.

a. *International Organization for Standardization.* ***(ISO 31000***
b. ***COBIT*** *(Control Objectives for Information and Related Technologies)*
c. ***ITIL*** *(Information Technology Infrastructure Library)*
d. ***RIMS*** *(Risk Maturity Model)*
e. ***COSO*** *(Committee of Sponsoring Organizations)*

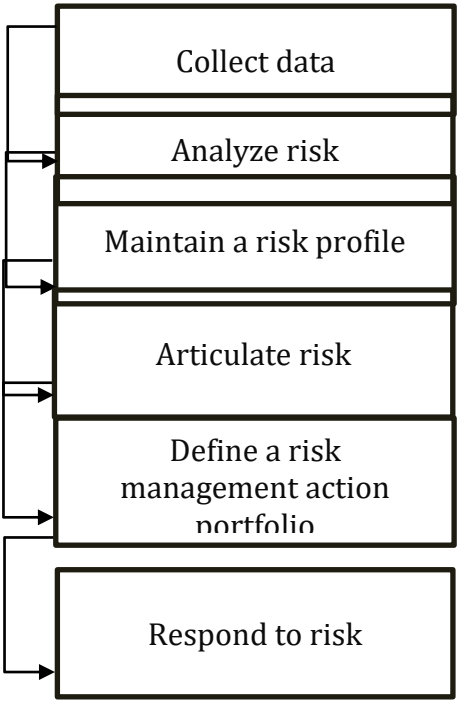
Pada proses manajemen Risiko secara umum terdiri dari 3 bagian utama yang terdiri dari;

a. Risk Assesment
Tujuan dari proses ini akan dilakukan untuk mengidentifikasi area yang beresiko tinggi di perusahaan proses ini dapat dibentuk dengan menerapkan RBS sehingga dapat dipetakan level resiko, domain dan dampak dari resiko tersebut.

b. Risk Mitigation
Tujuan dari proses ini untuk melakukan pengendalian terhadap risiko yang telah teridentifikasi, semakin tinggi pengendalian risiko TI berdampak pada turunnya risiko namun akan meningkat pada pembiayaan. Sehingga saat mengidentifikasi pengendalian harus memperhatikan pembiayaan juga.

c. Risk Evaluation
Setelah melewati kedua proses tersebut dalam fase waktu yang ditentukan, maka lakukanlah evaluasi terkait dengan identifikasi risiko dan proses mitigasi yang dilakukan apakah sudah sesuai atau belum dalam pengendalaian risiko terhadap risiko yang terjadi dan apakah dapat menekan biaya yang dikeluarkan untuk pengendalian risiko.

Untuk menerapkan ketiga proses diatas secara detail maka dapat menggunakan tahapan manajemen risiko dari salah satu framework. Dalam penulisan ini digunakan contoh tahapan dari *Framwork Cobit* dengan *Domain APO 12 Managed Risk* yang digambarkan pada gambar 5. (Information Systems Audit and Control Association., n.d.)



Gambar 9.5. *Domain APO 12 Managed Risk*
(Sumber : COBIT 2019)

a. *Collect Data*
   Pada tahap ini dilakukan identifikasi dan pengumpulan data untuk mengaktifkan risiko yang terkait dengan TI

yang efektif, proses ini dilakukan dengan mengidentifikasi, analisis hingga pelaporan.

Ada 8 aktivitas utama yang harus dikerjakan pada proses ini yang ditertuang pada tabel 9.1.

Tabel 9.1. Aktivitas Pengumpulan Data

No.	Aktivitas
1.	Melakukan proses penetapan dan penentuan metode untuk melakukan pengumpulan, klasifikasi, dan analisis data terkait dengan risiko TI.
2.	Melakukan rekapan terkait risiko TI yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan atau organisasi.
3.	Mengadopsi atau menentukan taksonomi risiko untuk mendefinisikan skenario risiko, kategori dampak dan kemungkinan.
4.	Melakukan pencatatan data terkait risiko TI yang menyebabkan atau dapat menyebabkan dampak bagi bisnis sesuai dengan kategori dampak yang ditentukan pada taksonomi risiko. Kemudian melakukan rekapan Rekap data dengan baik terkait dengan masalah yang telah terjadi.
5.	Melakukan Survei dan analisis data risiko TI secara historis dan mencatat pengalaman kerugian dari data dan tren yang tersedia secara eksternal melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa risiko secara umum.
6.	Atur data yang dikumpulkan dan tandai faktor yang berkontribusi. Tentukan kontribusi umum faktor di berbagai peristiwa.
7.	Menentukan kondisi spesifik yang ada atau tidak ada saat kejadian risiko terjadi dan lihat bagaimana kondisi

No.	Aktivitas
	tersebut berpengaruh pada frekuensi kejadian dan besarnya kerugian.
8.	Melakukan analisis peristiwa dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang akan muncul dan untuk mendapatkan pemahaman tentang terkait dengan faktor risiko internal maupun eksternal.

b. Analyze Risk

Pada tahap ini dilakukan pengembangan pandangan yang kuat dan lebih dalam tentang risiko TI secara aktual, untuk mendukung keputusan risiko. Pada proses ini terdapat 8 aktivitas utama yang harus dikerjakan.

Tabel 9.2. Analisis Risiko

No.	Akitivitas
1.	Menentukan ruang lingkup terkait uupaya analisis risiko yang sesuai, dengan melakukan pertimbangan pada semua faktor risiko dan/atau kekritisan aset bisnis
2.	Membangun atau memperbaharui skenario risiko TI secara berkala dan teratur, paparkan skenario mengenai level risiko dan kerugian terkait TI, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang mengalir dan/atau kebetulan. Kembangkan pengendalian untuk kontrol khusus kegiatan dan kembangkan kemampuan untuk mendeteksi.
3.	Perkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Memperhitungkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.
4.	Bandingkan risiko saat ini (eksposur kerugian terkait TI)

No.	Akitivitas
	dengan level dan toleransi risiko yang dapat diterima.
5.	Usulkan tanggapan risiko untuk risiko yang melebihi selera risiko dan tingkat toleransi.
6.	Tentukan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Mengidentifikasi persyaratan dan ekspektasi untuk kontrol kunci yang sesuai untuk respons mitigasi risiko
7.	Validasi hasil analisis risiko dan analisis dampak bisnis sebelum digunakan dalam pengambilan keputusan. Konfirmasikan bahwa analisis selaras dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti.
8.	Menganalisis biaya/manfaat opsi respons risiko potensial seperti menghindari, mengurangi, mentransfer/membagikan, dan menerima dan mengeksploitasi/merampas. Konfirmasikan respons risiko yang optimal.

c. Maintain a risk profile

Pada tahap ini dilakukan untuk Menjaga inventarisasi risiko yang telah diketahui dan atribut risiko, termasuk frekuensi yang diharapkan, potensi dampak dan tanggapan. Dokumen terkait sumber daya, kapabilitas, dan pengendalian aktivitas saat ini terkait dengan risiko item. Pada tahap terdapat 7 aktivitas utama.

Tabel 9.3. Pertahankan profil risiko

No.	Aktivitas
1.	Menginventarisasi proses bisnis dan mendokumentasikan ketergantungannya pada proses manajemen layanan TI dan infrastruktur sumber daya TI. Identifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan agen *outsourcing*
2.	Menentukan dan menyepakati layanan TI dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan operasi bisnis proses. Menganalisis dependensi dan mengidentifikasi tautan yang lemah.
3.	Penilaian skenario risiko berdasarkan kategori, lini bisnis, dan area fungsional
4.	Rekap semua informasi profil risiko dan gabungkan ke dalam profil risiko gabungan secara teratur.
5.	Tangkap informasi tentang status rencana tindakan risiko untuk disertakan dalam profil risiko TI perusahaan
6.	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan pemantauan cepat risiko saat ini dan tren risiko.
7.	Rekap informasi tentang peristiwa risiko TI yang telah terwujud untuk dimasukkan dalam profil risiko TI perusahaan.

d. Articulate risk.

Pada tahap ini dilakukan untuk mengkomunikasikan informasi tentang keadaan paparan TI saat ini dan peluang secara tepat waktu untuk semua pemangku kepentingan

yang diperlukan dengan tanggapan yang sesuai. Pada proses ini terdapat 5 aktivitas utama.

Tabel 9.4. Mengartikulasikan risiko

No.	Aktivitas
1.	Laporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan kisaran kerugian atau keuntungan bersama dengan tingkat kepercayaan, agar manajemen dapat melakukan penyeimbangan pengembalian risiko.
2.	Memberi para pembuat keputusan pemahaman tentang skenario terburuk dan skenario paling mungkin, paparan kerugian terkait TI, dan reputasi yang signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai dengan taksonomi risiko.
3.	Laporkan profil risiko saat ini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas kontrol, kesenjangan, inkonsistensi, redudansi, status perbaikan dan dampaknya terhadap profil risiko.
4.	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, identifikasi peluang terkait TI yang memungkinkan penerimaan risiko yang lebih besar dan peningkatan pertumbuhan dan pengembalian.
5.	Tinjau hasil penilaian pihak ketiga yang objektif dan tinjauan audit internal dan jaminan kualitas. Sertakan mereka di profil risiko. Tinjau kesenjangan

No.	Aktivitas
	yang teridentifikasi dan eksposur kerugian terkait I&T untuk menentukan kebutuhan akan analisis risiko tambahan.

e. Define a risk management action portfolio.
Pada tahap ini digunakan untuk melakukan Kelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima atau disajikan sebagai portofolio.

Tabel 9.5. Mendefenisikan portofolio manajemen resiko

No.	Aktivitas
1.	Menjaga inventarisasi aktivitas pengendalian yang ada untuk memitigasi risiko dan yang memungkinkan risiko diambil sejalan toleransi pengendalian risiko. Mengklasifikasikan aktivitas kontrol dan memetakannya ke skenario risiko TI tertentu.
2.	Tentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam individu dan tingkat toleransi portofolio.
3.	Tentukan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan perusahaan strategis peluang, dengan mempertimbangkan biaya, manfaat, efek pada profil risiko dan peraturan saat ini.

f. Respond to risk
Pada tahap ini dilakukan komunikasi informasi tentang keadaan paparan terkait TI saat ini dan peluang secara tepat

waktu untuk semua pemangku kepentingan yang diperlukan untuk respons yang sesuai. Pada tahap ini terdapat 5 kegiatan utama.

Tabel 9.6. Menanggapi Risiko

No.	Aktivitas
1.	Siapkan, pertahankan, dan uji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan operasional yang signifikan atau insiden pembangunan dengan dampak bisnis yang serius. Pastikan bahwa rencana mencakup jalur eskalasi di seluruh perusahaan
2.	Terapkan rencana respons yang tepat untuk meminimalkan dampak ketika insiden risiko terjadi.
3.	Mengkategorikan insiden dan membandingkan eksposur kerugian terkait TI dengan ambang batas toleransi risiko. Komunikasikan dampaknya bagi proses bisnis kepada pengambil keputusan sebagai bagian dari pelaporan dan pembaruan profil risiko.
4.	Periksa peristiwa/kerugian masa lalu yang merugikan dan peluang yang terlewatkan serta tentukan akar penyebabnya.
5.	Komunikasikan akar penyebab, persyaratan respons risiko tambahan, dan perbaikan proses kepada pembuat keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan peningkatan proses disertakan dalam proses tata kelola risiko.

DAFTAR PUSTAKA

Hairul, 2020.

Information Systems Audit and Control Association., n.d. COBIT 2019 Framework Governance and Management Objectives.
ISO 38500, 2008. Corporate governance of information technology Gouvernance des technologies de l'information par l'entreprise.
Paul Hopkin, 2017. Fundamentals of Risk Management.
Risma, 2021. Manajemen Resiko Teknologi Informasi

BAB 10
PENETAPAN IT YANG EFEKTIF DAN LINGKUNGAN KEAMANAN

Oleh Agung Susilo Yuda Irawan

10.Pendahuluan

Penggunaan teknologi informasi (IT) semakin meluas di seluruh dunia dan telah menjadi bagian integral dari operasi bisnis modern. Namun, dengan meningkatnya ketergantungan pada IT, keamanan informasi semakin menjadi perhatian penting. Penetapan IT yang efektif dan lingkungan keamanan yang kuat adalah kunci untuk menjaga keberhasilan dan keberlanjutan bisnis (Hariyono, 2018).

10.2 Memahami Risiko Keamanan IT

Memahami risiko keamanan IT adalah langkah penting dalam menetapkan lingkungan keamanan yang efektif untuk organisasi. Risiko keamanan IT dapat didefinisikan sebagai kemungkinan terjadinya kerugian atau gangguan pada sistem atau data IT yang disebabkan oleh ancaman keamanan seperti serangan hacker, virus, kegagalan sistem, atau kesalahan manusia.

Beberapa contoh risiko keamanan IT yang umum meliputi:

- Kehilangan data yang sensitif atau penting akibat kebocoran, peretasan atau kesalahan manusia
- Gangguan operasi bisnis akibat kegagalan sistem atau serangan malware
- Penyalahgunaan akses oleh pengguna yang tidak berwenang atau aktivitas ilegal di dalam system

- Pencurian identitas atau informasi pribadi oleh pihak yang tidak berwenang
- Kebocoran informasi rahasia perusahaan kepada pesaing atau pihak yang tidak berwenang.

Untuk mengidentifikasi risiko keamanan IT, organisasi harus melakukan penilaian risiko secara teratur. Langkah-langkah dalam penilaian risiko meliputi:

- Mengidentifikasi aset IT, yaitu semua data dan sistem yang harus dilindungi
- Mengidentifikasi ancaman keamanan yang mungkin terjadi pada aset IT
- Mengukur tingkat kerentanan atau kelemahan dalam sistem IT yang memungkinkan ancaman tersebut terjadi
- Menghitung dampak finansial atau operasional yang mungkin terjadi jika risiko terjadi.

Setelah risiko keamanan IT diidentifikasi dan diukur, organisasi dapat mengembangkan rencana tindakan untuk mengurangi atau mengelola risiko tersebut. Ini termasuk mengimplementasikan kebijakan keamanan yang tepat, melatih karyawan dalam penggunaan sistem dan prosedur keamanan, serta memastikan bahwa sistem IT terus diperbarui dan ditingkatkan untuk mengatasi ancaman keamanan yang terus berkembang (Khoironi, 2020).

10.2.1 Mengidentifikasi ancaman & risiko keamanan IT

Mengidentifikasi ancaman dan risiko keamanan IT merupakan langkah penting dalam menetapkan lingkungan keamanan IT yang efektif untuk organisasi. Ancaman keamanan IT adalah kemungkinan terjadinya kejadian yang merugikan pada sistem IT, sedangkan risiko keamanan IT adalah tingkat keparahan dari ancaman tersebut. Beberapa contoh ancaman keamanan IT meliputi:

1. Malware: Program jahat seperti virus, worm, trojan, atau spyware yang dapat merusak, mencuri atau merusak data pada sistem IT.
2. Serangan DoS/DDoS: Serangan Denial-of-Service (DoS) dan Distributed-Denial-of-Service (DDoS) dapat membuat sistem IT menjadi tidak dapat diakses atau beroperasi, mengganggu bisnis dan merugikan organisasi.
3. Peretasan: Upaya untuk mengakses sistem IT secara tidak sah dengan tujuan mencuri data atau merusak sistem.
4. Pencurian identitas: Upaya untuk mencuri informasi pribadi atau rahasia organisasi, seperti username, password, nomor kartu kredit, atau nomor identitas lainnya.
5. Kelemahan dalam sistem: Kelemahan dalam sistem IT, seperti perangkat keras atau perangkat lunak yang usang atau tidak diperbarui secara teratur, dapat menyebabkan risiko keamanan yang lebih tinggi.

Untuk mengidentifikasi ancaman keamanan IT, organisasi harus melakukan analisis dan penilaian risiko secara teratur. Hal ini meliputi:

- Identifikasi aset IT yang harus dilindungi
- Identifikasi ancaman keamanan yang mungkin terjadi pada aset IT
- Mengukur tingkat kerentanan atau kelemahan dalam sistem IT yang memungkinkan ancaman tersebut terjadi
- Menghitung dampak finansial atau operasional yang mungkin terjadi jika risiko terjadi.

Dengan cara ini, organisasi dapat mengembangkan rencana tindakan untuk mengurangi atau mengelola risiko keamanan IT. Hal ini meliputi mengimplementasikan kebijakan keamanan yang tepat, melatih karyawan dalam penggunaan sistem dan prosedur keamanan, serta memastikan bahwa

sistem IT terus diperbarui dan ditingkatkan untuk mengatasi ancaman keamanan yang terus berkembang (Matondang, 2018).

10.2.2 Memahami dampak keamanan IT yang tidak terkendali

Dampak keamanan IT yang tidak terkendali dapat sangat merugikan bagi organisasi dan penggunaannya. Beberapa dampak negatif yang dapat terjadi akibat keamanan IT yang tidak terkendali meliputi:

1. Kehilangan data: Ancaman seperti serangan malware atau peretasan dapat menyebabkan kehilangan data yang penting bagi organisasi. Data yang hilang dapat berupa data keuangan, data pelanggan, atau data operasional yang penting untuk kelangsungan bisnis.
2. Biaya yang tidak terduga: Ancaman keamanan IT yang tidak terkendali dapat menyebabkan biaya yang tidak terduga bagi organisasi. Biaya ini dapat berasal dari pemulihan data yang hilang, biaya pemulihan sistem yang terkena serangan, atau biaya kehilangan reputasi yang dapat mempengaruhi bisnis dan kepercayaan pelanggan.
3. Gangguan operasional: Serangan DoS atau DDoS dapat mengganggu operasi organisasi dengan membuat sistem IT menjadi tidak dapat diakses. Ini dapat mempengaruhi kemampuan organisasi untuk menjalankan bisnisnya, mengakses data yang penting, atau memberikan layanan kepada pelanggan.
4. Pelanggaran data pribadi: Jika organisasi tidak dapat menjaga keamanan data pribadi seperti nomor kartu kredit atau nomor identitas, maka organisasi dapat terkena sanksi atau denda karena pelanggaran privasi data.
5. Hilangnya kepercayaan pelanggan: Keamanan IT yang buruk dapat mempengaruhi kepercayaan pelanggan dan merusak

reputasi organisasi. Jika pelanggan tidak merasa aman memberikan informasi pribadi atau data transaksinya, maka mereka mungkin akan mencari penyedia layanan yang lebih aman dan dapat dipercaya.

Dalam beberapa kasus, dampak keamanan IT yang buruk dapat sangat merugikan bagi organisasi sehingga bisnis tidak dapat lagi beroperasi. Oleh karena itu, penting bagi organisasi untuk mengambil langkah-langkah yang tepat untuk mengidentifikasi, mengelola, dan mengurangi risiko keamanan IT. Hal ini dapat membantu organisasi untuk menjaga keamanan data mereka, melindungi reputasi mereka, dan memastikan kelangsungan bisnis yang berkelanjutan (Muthoharoh, 2021).

10.2.3 Mengukur Tingkat Risiko IT dalam Organisasi

Untuk mengukur tingkat risiko keamanan IT dalam sebuah organisasi, dapat dilakukan beberapa langkah sebagai berikut:

1. Identifikasi aset-aset IT yang penting: Identifikasi aset-aset IT yang paling penting bagi organisasi, seperti data pelanggan, data keuangan, atau sistem kritis. Ini akan membantu dalam menentukan risiko-risiko yang terkait dengan aset-aset ini.
2. Identifikasi ancaman dan kerentanan: Identifikasi ancaman-ancaman yang dapat mempengaruhi keamanan aset-aset IT, seperti serangan malware, serangan DDoS, atau peretasan. Selanjutnya, identifikasi kerentanan-kerentanan yang dapat dimanfaatkan oleh para penyerang untuk mengeksploitasi aset-aset IT.
3. Penilaian risiko: Gunakan kerangka kerja penilaian risiko untuk menilai potensi kerugian dan dampak keamanan dari ancaman dan kerentanan yang telah diidentifikasi. Penilaian

risiko dapat dilakukan dengan mempertimbangkan probabilitas terjadinya ancaman dan kerentanan, serta dampak yang mungkin terjadi jika terjadi pelanggaran keamanan.

4. Penetapan prioritas: Setelah melakukan penilaian risiko, organisasi dapat menentukan prioritas untuk mengurangi risiko yang terkait dengan aset-aset IT tertentu. Prioritas dapat ditentukan berdasarkan dampak yang mungkin terjadi, kemungkinan terjadinya ancaman atau kerentanan, dan biaya untuk mengurangi risiko.
5. Pelaporan: Pelaporan hasil penilaian risiko dan upaya mitigasi risiko yang dilakukan adalah langkah penting untuk memastikan bahwa manajemen dan stakeholder organisasi memahami risiko dan upaya yang dilakukan untuk mengurangi risiko keamanan IT.

Dalam melakukan penilaian risiko keamanan IT, penting untuk melibatkan berbagai bagian dari organisasi, seperti tim keamanan IT, manajemen senior, dan bagian-bagian fungsional yang terkait dengan aset-aset IT. Dengan cara ini, organisasi dapat memiliki pemahaman yang lebih baik tentang risiko keamanan IT yang dihadapinya dan dapat mengambil tindakan yang tepat untuk mengurangi risiko tersebut (Misbah, 2017).

10.3 Penetapan IT yang Efektif

Penetapan IT yang efektif adalah proses yang dilakukan oleh sebuah organisasi untuk memastikan bahwa teknologi informasi (IT) digunakan secara optimal untuk mendukung tujuan bisnis jangka panjang organisasi. Proses ini melibatkan beberapa langkah penting yang harus dilakukan dengan terencana dan sistematis.

Pertama-tama, organisasi harus menentukan kebutuhan dan tujuan IT. Ini melibatkan pemahaman yang baik tentang proses bisnis organisasi dan tujuan bisnis jangka panjang. Dalam langkah ini, organisasi harus memastikan bahwa kebutuhan dan tujuan IT terkait erat dengan tujuan bisnis jangka panjang, sehingga IT dapat menjadi alat untuk mencapai tujuan tersebut.

Setelah kebutuhan dan tujuan IT ditentukan, organisasi harus membuat strategi IT yang efektif untuk memenuhi kebutuhan dan mencapai tujuan. Strategi ini harus mencakup rencana jangka panjang dan jangka pendek, serta harus selaras dengan rencana bisnis organisasi.

Langkah berikutnya adalah mengembangkan rencana kerja IT yang jelas. Rencana kerja ini harus mencakup rincian tentang tugas dan tanggung jawab serta waktu yang dihabiskan untuk setiap tugas. Hal ini akan membantu memastikan bahwa implementasi strategi IT berjalan dengan lancar dan efektif.

Terakhir, organisasi harus menilai dan memilih teknologi yang tepat untuk memenuhi kebutuhan dan mencapai tujuan IT. Proses pemilihan teknologi harus didasarkan pada evaluasi yang cermat tentang teknologi yang tersedia dan kebutuhan IT organisasi. Selain itu, organisasi harus memastikan bahwa teknologi yang dipilih dapat diimplementasikan dengan lancar dan dapat dikelola secara efektif.

Dalam rangka mencapai penetapan IT yang efektif, organisasi harus memastikan bahwa keempat langkah tersebut dijalankan dengan baik dan terus-menerus dievaluasi dan ditingkatkan sesuai dengan perkembangan bisnis dan teknologi. Dengan demikian, organisasi dapat memanfaatkan IT secara optimal dan efektif untuk mencapai tujuan bisnis jangka Panjang (Pardani, 2017).

10.3.1 Menentukan Kebutuhan dan Tujuan IT

Menentukan kebutuhan dan tujuan IT merupakan langkah kritis dalam penetapan IT yang efektif. Hal ini melibatkan pemahaman terhadap proses bisnis organisasi dan tujuan bisnis jangka panjang, sehingga IT dapat menjadi alat untuk mencapai tujuan tersebut.

Berikut adalah langkah-langkah yang dapat dilakukan untuk menentukan kebutuhan dan tujuan IT:

1. Analisis proses bisnis: Analisis proses bisnis membantu organisasi untuk memahami bagaimana bisnis mereka beroperasi dan bagaimana IT dapat membantu untuk meningkatkan efisiensi dan produktivitas. Hal ini melibatkan pemetaan proses bisnis, menentukan input dan output dari setiap proses, dan mengidentifikasi area yang memerlukan perubahan.
2. Identifikasi kebutuhan bisnis: Setelah proses bisnis dipahami, organisasi harus mengidentifikasi kebutuhan bisnis spesifik yang dapat dipenuhi dengan IT. Hal ini meliputi pengidentifikasian masalah atau tantangan yang harus diatasi, pengenalan peluang baru, dan mempertimbangkan faktor-faktor seperti regulasi atau persyaratan keamanan.
3. Tentukan tujuan IT yang jelas: Setelah kebutuhan bisnis diidentifikasi, organisasi harus menentukan tujuan IT yang jelas yang terkait dengan tujuan bisnis jangka panjang. Tujuan ini harus terukur dan dapat dicapai dalam jangka waktu tertentu.4
4. Prioritaskan kebutuhan: Setelah kebutuhan dan tujuan ditentukan, organisasi harus memprioritaskan kebutuhan berdasarkan urgensi dan dampak pada tujuan bisnis. Ini akan membantu organisasi untuk memfokuskan sumber daya dan anggaran pada area yang paling penting.

5. Libatkan stakeholder: Penting untuk melibatkan stakeholder dalam menentukan kebutuhan dan tujuan IT. Stakeholder dapat memberikan masukan dan memastikan bahwa kebutuhan mereka terpenuhi.

Dengan memahami kebutuhan dan tujuan IT, organisasi dapat memilih solusi teknologi yang tepat untuk mencapai tujuan bisnis mereka dan memaksimalkan penggunaan IT dalam operasi bisnis mereka (Ikhwan, 2020).

10.3.2 Membuat IT Strategi yang Efektif

Membuat strategi IT yang efektif merupakan langkah penting dalam penetapan IT yang efektif. Strategi ini harus mencakup rencana jangka panjang dan jangka pendek untuk memenuhi kebutuhan IT organisasi serta selaras dengan rencana bisnis jangka panjang organisasi.

Dalam pembuatan strategi IT, organisasi harus mempertimbangkan beberapa faktor, seperti perkembangan teknologi informasi, kebutuhan dan tujuan bisnis, dan ketersediaan sumber daya. Selain itu, organisasi juga harus mempertimbangkan faktor risiko dan keamanan dalam penggunaan teknologi informasi (Agustina, 2020) .

10.3.3 Mengembangkan Rencana Kerja IT yang jelas

Setelah membuat strategi IT yang efektif, langkah selanjutnya dalam penetapan IT yang efektif adalah mengembangkan rencana kerja IT yang jelas. Rencana kerja ini akan menjadi panduan dalam mengimplementasikan strategi IT dan mencapai tujuan bisnis yang telah ditetapkan.

Rencana kerja IT yang jelas harus mencakup langkah-langkah spesifik yang akan diambil dalam mengimplementasikan strategi IT, termasuk jadwal waktu, sumber daya yang dibutuhkan, anggaran, dan tanggung jawab

tim. Tim IT harus terlibat dalam pengembangan rencana kerja ini dan memastikan bahwa rencana kerja tersebut realistis dan dapat dijalankan.

Selain itu, rencana kerja IT juga harus mencakup upaya untuk mengidentifikasi dan mengatasi risiko yang mungkin timbul selama implementasi strategi IT. Upaya untuk memitigasi risiko harus diintegrasikan ke dalam rencana kerja dan harus diberikan prioritas tinggi untuk memastikan keberhasilan implementasi strategi IT.

Secara keseluruhan, mengembangkan rencana kerja IT yang jelas adalah langkah penting dalam penetapan IT yang efektif. Rencana kerja ini akan membantu organisasi memastikan bahwa strategi IT dapat diimplementasikan dengan sukses dan mencapai tujuan bisnis yang telah ditetapkan (Simarmata, 2020).

10.3.4 Menilai dan Memilih teknologi yang tepat

Setelah menentukan kebutuhan dan tujuan IT, membuat strategi IT yang efektif, dan mengembangkan rencana kerja IT yang jelas, langkah selanjutnya dalam penetapan IT yang efektif adalah menilai dan memilih teknologi yang tepat.

Proses evaluasi teknologi harus mempertimbangkan kebutuhan bisnis dan harus dilakukan dengan hati-hati. Beberapa faktor yang perlu dipertimbangkan termasuk kemampuan teknologi dalam memenuhi kebutuhan bisnis, biaya, dan faktor keamanan.

Pertimbangan lainnya meliputi fleksibilitas teknologi dan kemampuan untuk diintegrasikan dengan sistem yang sudah ada, serta ketersediaan dukungan teknis dan pelatihan. Jangan lupa untuk mempertimbangkan juga faktor risiko keamanan teknologi yang akan digunakan, dan memastikan bahwa teknologi yang dipilih memiliki tingkat keamanan yang memadai untuk melindungi informasi sensitif organisasi.

Setelah melakukan evaluasi teknologi yang cukup, organisasi dapat memilih teknologi yang tepat untuk memenuhi kebutuhan bisnis dan strategi IT yang telah ditetapkan. Namun, organisasi juga harus mempertimbangkan bahwa teknologi terus berkembang dan akan selalu ada teknologi baru yang muncul di masa depan. Oleh karena itu, organisasi harus tetap beradaptasi dan memperbarui teknologi mereka agar tetap efektif dan mengikuti tren terbaru (Ishak, 2020).

10.4 Kebijakan dan Prosedur Keamanan

Kebijakan dan prosedur keamanan merupakan bagian penting dari penetapan IT yang efektif. Kebijakan keamanan digunakan untuk menentukan standar keamanan dan aturan yang harus diikuti oleh seluruh karyawan dalam organisasi. Sedangkan prosedur keamanan merupakan langkah-langkah praktis yang harus diikuti untuk menjaga keamanan sistem dan data organisasi.

Kebijakan keamanan biasanya mencakup aturan terkait penggunaan perangkat lunak dan perangkat keras, akses ke jaringan dan data, password, backup dan pemulihan, serta pengelolaan dan pemantauan sistem keamanan. Tujuan dari kebijakan keamanan adalah untuk memastikan bahwa semua orang dalam organisasi memahami pentingnya keamanan dan bertanggung jawab atas tindakan mereka terhadap keamanan.

Sementara itu, prosedur keamanan meliputi tindakan praktis yang harus dilakukan oleh karyawan untuk menjaga keamanan. Misalnya, prosedur keamanan bisa mencakup verifikasi penggunaan password yang kuat dan unik, backup data secara teratur, penggunaan perangkat lunak keamanan yang terbaru, dan penghapusan data secara aman jika tidak diperlukan lagi.

Kebijakan dan prosedur keamanan yang efektif akan membantu melindungi organisasi dari ancaman keamanan, serta meminimalkan risiko kehilangan atau pencurian data. Namun, penting untuk diingat bahwa kebijakan dan prosedur keamanan harus diterapkan dan dipatuhi oleh seluruh karyawan dalam organisasi agar efektif. Oleh karena itu, pelatihan dan komunikasi yang tepat sangat penting dalam implementasi kebijakan dan prosedur keamanan (Darwis, 2021).

10.4.1 Membuat Kebijakan Keamanan IT

Membuat kebijakan keamanan IT adalah proses untuk menetapkan standar dan prosedur untuk melindungi sistem, jaringan, dan data dari ancaman keamanan. Hal ini meliputi identifikasi dan evaluasi risiko keamanan, dan menetapkan tindakan yang diperlukan untuk mengurangi atau menghilangkan risiko tersebut.

Penting untuk mengingat bahwa kebijakan keamanan IT tidaklah statis, dan harus diperbarui secara teratur sesuai dengan perubahan dalam lingkungan bisnis dan teknologi informasi. Oleh karena itu, pastikan bahwa kebijakan dan prosedur keamanan IT diupdate secara berkala untuk memastikan bahwa organisasi selalu memiliki tingkat keamanan yang optimal (Ramadhani, 2020).

10.4.2 Mengembangkan Prosedur Keamanan Yang Efektif

Mengembangkan prosedur keamanan yang efektif adalah langkah penting dalam menjaga keamanan sistem dan data dalam lingkungan IT sebuah organisasi. Prosedur keamanan yang baik harus mencakup tindakan preventif dan responsif terhadap ancaman keamanan seperti serangan siber, kehilangan data, dan kebocoran informasi. Berikut adalah beberapa langkah yang dapat dilakukan dalam mengembangkan prosedur keamanan yang efektif:

1. Identifikasi risiko keamanan: Langkah pertama dalam mengembangkan prosedur keamanan yang efektif adalah dengan mengidentifikasi risiko keamanan yang mungkin timbul di lingkungan IT organisasi. Risiko keamanan dapat berasal dari berbagai sumber seperti serangan siber, kesalahan manusia, bencana alam, atau kegagalan perangkat keras.
2. Penetapan kebijakan keamanan: Setelah mengidentifikasi risiko keamanan, langkah berikutnya adalah menetapkan kebijakan keamanan untuk mengurangi atau menghilangkan risiko tersebut. Kebijakan keamanan dapat mencakup hal-hal seperti penggunaan sandi yang kuat, hak akses yang terbatas, dan penyimpanan data yang aman.
3. Penetapan prosedur keamanan: Setelah menetapkan kebijakan keamanan, langkah selanjutnya adalah membuat prosedur keamanan yang jelas dan mudah diikuti oleh seluruh pengguna sistem. Prosedur keamanan harus mencakup hal-hal seperti penggunaan perangkat lunak keamanan, penanganan data yang sensitif, dan pengaturan sandi secara berkala.
4. Pelatihan dan pengawasan: Pelatihan dan pengawasan yang tepat dapat membantu memastikan bahwa prosedur keamanan diikuti dengan benar oleh seluruh pengguna sistem. Pelatihan harus meliputi penggunaan perangkat lunak keamanan, penanganan data yang sensitif, dan pengaturan sandi yang kuat. Pengawasan dapat dilakukan melalui pemeriksaan rutin oleh tim keamanan atau penggunaan perangkat lunak pemantauan keamanan.

Evaluasi dan pembaruan: Terakhir, prosedur keamanan harus dievaluasi secara berkala untuk memastikan bahwa tetap efektif dalam menghadapi risiko keamanan yang baru muncul. Jika diperlukan, prosedur keamanan harus diperbarui untuk

mengakomodasi perubahan dalam teknologi dan ancaman keamanan (Setyoko, 2019).

10.5 Pengelolaan Identitas dan Akses

Pengelolaan identitas dan akses merupakan salah satu aspek penting dalam penetapan IT yang efektif dan lingkungan keamanan. Hal ini berkaitan dengan cara organisasi mengelola akses dan penggunaannya oleh pengguna atau karyawan, baik dalam hal sistem IT maupun aplikasi bisnis lainnya.

Pengelolaan identitas dan akses melibatkan proses otentikasi dan otorisasi. Proses otentikasi digunakan untuk memverifikasi identitas pengguna dan memastikan bahwa hanya orang yang tepat yang memiliki akses ke sistem dan informasi. Sedangkan proses otorisasi digunakan untuk memastikan bahwa pengguna hanya memiliki akses ke informasi atau sumber daya yang diperlukan dalam pekerjaannya.

Untuk menjaga keamanan IT, organisasi harus memiliki kebijakan yang jelas dan prosedur pengelolaan identitas dan akses yang efektif. Kebijakan ini harus mencakup hal-hal seperti penerapan kata sandi yang kuat, pembatasan akses pada tingkat yang sesuai dengan tanggung jawab pekerjaan, serta pelaporan kejadian yang mencurigakan atau tidak terduga pada sistem IT.

10.5.1 Mengelola Identitas dan Akses Pengguna

Pengelolaan identitas dan akses pengguna adalah proses yang dilakukan untuk mengatur akses pengguna ke dalam sistem informasi. Hal ini meliputi pengelolaan identitas pengguna, termasuk pembuatan, penghapusan, dan perubahan informasi identitas. Selain itu, proses ini juga mencakup pemberian dan penghapusan hak akses pengguna untuk mengakses sistem informasi yang ada.

Dalam pengelolaan identitas dan akses pengguna, penting untuk menentukan level akses yang sesuai. Hal ini berarti memberikan hak akses yang tepat pada tingkat kebutuhan bisnis. Sebagai contoh, seorang karyawan hanya perlu memiliki akses ke data yang relevan dengan pekerjaannya, sementara manajer harus memiliki hak akses yang lebih luas untuk mengelola operasi bisnis. Selain itu, untuk memastikan akses yang aman, otentikasi dan otorisasi yang tepat harus diterapkan. Otentikasi adalah proses verifikasi identitas pengguna yang dilakukan sebelum diberikan hak akses, sementara otorisasi mengacu pada hak akses yang diberikan kepada pengguna setelah identitasnya terverifikasi.

Terakhir, memonitor aktivitas pengguna adalah bagian penting dari pengelolaan identitas dan akses pengguna. Hal ini dilakukan untuk mendeteksi aktivitas mencurigakan yang mungkin terjadi pada sistem informasi, seperti upaya pencurian data atau pelanggaran kebijakan keamanan. Monitor aktivitas pengguna harus dilakukan secara terus-menerus dan teratur, sehingga dapat mendeteksi risiko keamanan yang muncul dengan cepat dan tepat waktu. Dengan mengelola identitas dan akses pengguna dengan baik, organisasi dapat meminimalkan risiko keamanan dan memastikan bahwa hak akses diberikan dengan tepat, sesuai dengan kebutuhan bisnis dan standar keamanan (Putri, 2022).

10.5.2 Menentukan Level Akses Yang Sesuai

Menentukan level akses yang sesuai merupakan proses yang dilakukan untuk menentukan hak akses pengguna dalam menggunakan sistem informasi. Hal ini meliputi pengaturan tingkat akses pengguna terhadap data atau informasi tertentu, serta penentuan batasan akses terhadap fungsi atau aplikasi tertentu. Penentuan level akses yang sesuai bertujuan untuk

memastikan bahwa pengguna hanya memiliki akses yang sesuai dengan tugas dan tanggung jawab mereka dalam organisasi.

Proses menentukan level akses yang sesuai juga harus mempertimbangkan tingkat keamanan yang dibutuhkan oleh sistem informasi. Pada umumnya, level akses dibagi menjadi beberapa tingkatan, seperti level administrator, level user, dan level guest. Setiap tingkat akses memiliki hak akses yang berbeda dan harus diberikan secara proporsional berdasarkan peran dan tanggung jawab pengguna.

Selain itu, memastikan akses yang aman dengan otentikasi dan otorisasi yang tepat juga merupakan bagian penting dari pengelolaan identitas dan akses pengguna. Otentikasi adalah proses verifikasi identitas pengguna, sedangkan otorisasi adalah proses penentuan hak akses pengguna setelah otentikasi berhasil dilakukan. Sistem otentikasi dan otorisasi yang tepat dapat memastikan bahwa hanya pengguna yang sah yang memiliki akses ke sistem informasi, sehingga dapat mengurangi risiko keamanan dan melindungi informasi organisasi dari akses yang tidak sah (Ikhsan, 2019).

10.5.3 Memastikan akses yang aman dengan otentikasi dan otorisasi yang tepat

Memastikan akses yang aman dengan otentikasi dan otorisasi yang tepat adalah proses yang dilakukan untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem informasi dan sumber daya yang terkait. Hal ini meliputi proses autentikasi pengguna dengan menggunakan identitas dan sandi yang unik, serta proses otorisasi yang menentukan hak akses pengguna dalam sistem informasi. Proses ini juga melibatkan implementasi kontrol keamanan

yang tepat untuk melindungi informasi yang sensitif dan mengurangi risiko akses yang tidak sah.

Selain itu, dalam memastikan akses yang aman, diperlukan penerapan kebijakan keamanan yang ketat, seperti kebijakan sandi yang kuat, kebijakan pergantian sandi secara berkala, serta pembatasan upaya login yang gagal. Selain itu, pemantauan dan audit secara teratur juga diperlukan untuk memastikan bahwa sistem dan sumber daya TI terus terlindungi dengan baik.

Selain keamanan teknis, pengguna juga perlu dilatih dan diingatkan tentang pentingnya menjaga kerahasiaan informasi serta menjaga keamanan akun dan sandi mereka. Hal ini dapat dilakukan dengan memberikan pelatihan dan edukasi secara rutin kepada pengguna tentang praktik keamanan TI yang baik dan potensi risiko keamanan yang dapat terjadi.

Dalam memonitor aktivitas pengguna, perlu dilakukan pemantauan terhadap aktivitas yang mencurigakan atau tidak biasa, seperti upaya login yang gagal secara berulang-ulang, pengaksesan data yang tidak sah, atau aktivitas yang tidak sesuai dengan tugas dan tanggung jawab pengguna. Dalam hal ini, diperlukan adanya sistem pemantauan dan audit yang memadai untuk mendukung proses pengawasan dan deteksi dini terhadap ancaman keamanan (Kusuma, 2021).

10.5.4 Memonitor aktivitas pengguna

Memonitor aktivitas pengguna adalah proses yang dilakukan untuk memantau aktivitas pengguna dalam sistem informasi. Hal ini meliputi pencatatan aktivitas pengguna, seperti login, logout, dan aktivitas yang dilakukan saat menggunakan sistem informasi. Tujuan dari proses ini adalah untuk mengidentifikasi dan mencegah aktivitas yang mencurigakan atau tidak sah, serta untuk memastikan bahwa

pengguna mengikuti kebijakan keamanan dan prosedur yang telah ditetapkan oleh organisasi.

Dengan memantau aktivitas pengguna, organisasi dapat memperoleh informasi yang berguna untuk mengidentifikasi tren dan pola perilaku pengguna, serta untuk mengevaluasi efektivitas kebijakan keamanan yang telah ditetapkan. Dalam hal terjadi insiden keamanan atau pelanggaran, log aktivitas pengguna dapat digunakan sebagai bukti dan membantu dalam penyelidikan insiden tersebut. Oleh karena itu, memonitor aktivitas pengguna merupakan bagian penting dari pengelolaan identitas dan akses pengguna, serta dari upaya menjaga keamanan dan integritas sistem informasi (Halim, 2019).

10.6 Keamanan Jaringan

Keamanan jaringan adalah serangkaian tindakan dan strategi untuk melindungi jaringan komputer dari ancaman dan serangan. Jaringan komputer dapat menjadi sasaran utama para peretas yang mencoba untuk mengakses informasi sensitif, merusak sistem, atau mencuri data. Oleh karena itu, penting bagi organisasi untuk memiliki keamanan jaringan yang kuat untuk melindungi sistem dan data mereka (Munawar, 2020).

10.6.1 Memastikan keamanan jaringan dengan firewall, VPN, dan teknologi keamanan jaringan lainnya

Memastikan keamanan jaringan adalah suatu hal yang sangat penting dalam lingkup keamanan informasi. Proses ini dilakukan dengan mengimplementasikan teknologi keamanan jaringan seperti firewall dan *Virtual Private Network* (VPN), serta teknologi keamanan jaringan lainnya yang tepat. Firewall digunakan untuk memonitor dan mengendalikan lalu lintas data yang masuk dan keluar dari jaringan, sementara VPN memastikan bahwa koneksi jaringan yang digunakan aman dan terenkripsi. Teknologi keamanan jaringan lainnya seperti

Intrusion Detection System (IDS) dan *Intrusion Prevention System* (IPS) juga dapat digunakan untuk mendeteksi dan mencegah serangan yang tidak diinginkan terhadap jaringan.

Selain mengimplementasikan teknologi keamanan jaringan yang tepat, membuat kebijakan keamanan jaringan yang jelas juga sangat penting. Hal ini mencakup pengaturan aturan dan prosedur keamanan yang harus diikuti oleh semua pengguna jaringan, termasuk dalam penggunaan perangkat dan akses ke sumber daya jaringan. Kebijakan keamanan jaringan yang jelas dapat membantu meningkatkan kesadaran pengguna tentang pentingnya keamanan jaringan dan memberikan pedoman untuk tindakan yang harus diambil dalam situasi yang berbeda.

Selanjutnya, melindungi jaringan dari serangan dan ancaman keamanan juga merupakan bagian penting dari proses keamanan jaringan. Hal ini mencakup penggunaan teknologi keamanan yang tepat dan pemantauan terus menerus terhadap jaringan untuk mendeteksi dan merespons serangan atau ancaman yang terjadi. Penggunaan teknologi keamanan yang tepat seperti antivirus, antispyware, dan antimalware dapat membantu mencegah masuknya malware atau virus ke dalam jaringan. Selain itu, pemantauan terus menerus terhadap jaringan juga dapat membantu mendeteksi serangan atau ancaman keamanan yang terjadi dan memungkinkan untuk mengambil tindakan yang tepat untuk mengatasinya (Yulianto, 2020).

10.6.2 Membuat kebijakan keamanan jaringan yang jelas

Membuat kebijakan keamanan jaringan yang jelas adalah penting untuk memastikan bahwa pengguna dan staf mengerti dan mengikuti standar keamanan yang telah ditetapkan oleh organisasi. Kebijakan keamanan jaringan harus mencakup hal-hal seperti persyaratan keamanan password,

pembatasan akses jaringan, serta pedoman dalam memanfaatkan teknologi keamanan jaringan. Kebijakan ini harus diterapkan secara konsisten dan diikuti oleh seluruh anggota organisasi untuk meminimalkan risiko serangan terhadap jaringan.

Melindungi jaringan dari serangan dan ancaman keamanan juga sangat penting untuk menjaga keamanan informasi dalam suatu organisasi. Proses ini meliputi pengimplementasian kontrol keamanan seperti enkripsi data, penggunaan sertifikat digital, serta pemantauan dan pembaruan perangkat lunak keamanan secara rutin. Selain itu, penting juga untuk memastikan bahwa jaringan dilindungi dari serangan DDoS (*Distributed Denial of Service*) dan serangan phishing melalui pelatihan dan kesadaran keamanan yang tepat kepada pengguna dan staf. Dengan mengimplementasikan kontrol keamanan dan membangun kesadaran keamanan yang kuat, organisasi dapat meminimalkan risiko serangan dan memastikan keamanan jaringan dan informasi yang terkait (Palinggi, 2019).

10.6.3 Melindungi jaringan dari serangan dan ancaman keamanan

Melindungi jaringan dari serangan dan ancaman keamanan adalah tugas penting dalam memastikan keamanan informasi organisasi. Beberapa cara untuk melindungi jaringan termasuk dengan mengimplementasikan teknologi keamanan jaringan seperti firewall, VPN, IDS, dan IPS. Selain itu, patching dan pengaturan keamanan yang ketat pada sistem jaringan juga harus dilakukan secara teratur. Pengguna harus dilatih untuk mengenali serangan keamanan seperti phishing dan malware, serta diingatkan untuk selalu mematuhi kebijakan keamanan jaringan yang telah ditetapkan. Selain itu, proses audit keamanan jaringan juga harus dilakukan secara teratur

untuk mengidentifikasi kelemahan dan memastikan bahwa sistem jaringan berada pada kondisi yang aman.

Penambahan teknologi enkripsi data pada jaringan juga bisa menjadi cara efektif untuk melindungi jaringan dari ancaman keamanan. Dengan menerapkan teknologi enkripsi, data yang dikirim dan diterima melalui jaringan akan diacak sehingga hanya dapat dibaca oleh pihak yang memiliki kunci enkripsi. Selain itu, implementasi tindakan pengamanan fisik seperti penggunaan kunci akses dan pengawasan akses ke ruangan server juga dapat membantu dalam memastikan keamanan jaringan. Jangan lupa pula untuk memiliki rencana penanganan keamanan jaringan yang jelas dan terstruktur untuk mengatasi serangan keamanan yang tidak terduga.

Selain teknologi keamanan jaringan dan kebijakan keamanan yang jelas, proses pelatihan dan kesadaran keamanan juga sangat penting dalam memastikan keamanan jaringan. Pengguna harus dilatih untuk mengenali tanda-tanda serangan keamanan dan cara menghindari serangan tersebut. Dalam hal ini, kesadaran keamanan dapat dianggap sebagai lapisan pertahanan pertama terhadap serangan keamanan. Selain itu, proses backup dan pemulihan data juga harus dilakukan secara teratur untuk memastikan bahwa data penting dapat dipulihkan jika terjadi kerusakan atau serangan pada jaringan. Proses pelaporan keamanan juga harus ditetapkan untuk memungkinkan pengguna melaporkan masalah keamanan yang mereka temui dan untuk memastikan bahwa masalah tersebut segera ditangani oleh tim keamanan jaringan (Bustami, 2020).

10.7 Pemulihan dan Penanganan Kejadian Keamanan

Pemulihan dan Penanganan Kejadian Keamanan (*Incident Response and Recovery*) adalah suatu proses yang dilakukan oleh tim keamanan IT untuk merespon dan memulihkan sistem yang terkena serangan atau insiden keamanan. Tujuan dari proses ini adalah untuk mengurangi dampak dari insiden keamanan, mempercepat waktu pemulihan sistem, dan mengurangi kerugian yang ditimbulkan. Pemulihan dan Penanganan Kejadian Keamanan dimulai dengan mendeteksi insiden keamanan, kemudian melakukan investigasi untuk mengidentifikasi sumber insiden dan dampak yang ditimbulkan. Setelah itu, tim keamanan IT akan mengambil tindakan yang tepat untuk menghentikan serangan dan memulihkan sistem yang terkena dampak insiden.

Selain itu, proses Pemulihan dan Penanganan Kejadian Keamanan juga melibatkan pengumpulan dan analisis data terkait insiden keamanan yang terjadi, sehingga dapat digunakan sebagai acuan untuk meningkatkan sistem keamanan IT pada masa yang akan datang. Oleh karena itu, penting bagi organisasi untuk memiliki prosedur yang jelas dan terstruktur dalam mengatasi insiden keamanan, serta melatih tim keamanan IT secara teratur untuk memastikan bahwa mereka siap merespon setiap insiden keamanan yang terjadi (Yulianto 2021).

10.7.1 Menyiapkan Rencana Pemulihan Keamanan IT

Pemulihan keamanan IT adalah proses yang dilakukan untuk memulihkan sistem informasi dan operasi bisnis setelah terjadi insiden keamanan. Hal ini meliputi membuat rencana pemulihan keamanan IT yang jelas, dengan tujuan untuk memastikan bahwa organisasi dapat merespons dengan cepat dan efektif terhadap kejadian keamanan. Rencana pemulihan keamanan IT harus mencakup prosedur untuk memulihkan

sistem informasi, mengatasi kerusakan atau kehilangan data, serta memastikan bahwa operasi bisnis dapat kembali berjalan seperti biasa.

Organisasi juga harus membuat prosedur untuk penanganan kejadian keamanan. Prosedur ini harus mencakup langkah-langkah yang harus diambil ketika terjadi kejadian keamanan, termasuk bagaimana untuk melaporkan insiden, bagaimana untuk mengevaluasi dampaknya, dan langkah-langkah yang harus diambil untuk mengatasi insiden tersebut. Prosedur penanganan kejadian keamanan juga harus mencakup bagaimana untuk berkomunikasi dengan pihak yang terlibat dalam insiden, termasuk staf internal, vendor, dan otoritas penegak hukum.

Selama proses penanganan kejadian keamanan, organisasi harus terus memonitor dan mengevaluasi tindakan yang dilakukan. Hal ini penting untuk memastikan bahwa prosedur yang telah ditetapkan efektif dan dapat ditingkatkan jika diperlukan. Setelah kejadian keamanan telah ditangani, organisasi harus melakukan evaluasi yang komprehensif untuk mengidentifikasi akar penyebab dan meningkatkan sistem keamanan IT berdasarkan hasil evaluasi. Hal ini dapat meliputi peningkatan teknologi keamanan, pengembangan prosedur penanganan kejadian keamanan, dan pelatihan staf untuk mengenali dan melaporkan insiden keamanan (Supriyanto, 2019).

10.7.2 Membuat prosedur untuk penanganan kejadian keamanan

Prosedur untuk penanganan kejadian keamanan adalah suatu panduan atau petunjuk yang dibuat untuk membantu organisasi merespons dengan cepat dan efektif terhadap insiden keamanan. Hal ini meliputi prosedur untuk mengumpulkan bukti-bukti, mengevaluasi dampak insiden,

mengisolasi dan mengidentifikasi sumber insiden, serta menyelesaikan masalah keamanan dan memulihkan sistem keamanan. Proses ini harus dilakukan dengan cepat dan tepat untuk meminimalkan dampak insiden keamanan terhadap operasi bisnis.

Prosedur penanganan kejadian keamanan juga harus mencakup pemberitahuan dan koordinasi dengan pihak internal dan eksternal, seperti manajemen organisasi, tim keamanan, penyedia layanan keamanan, dan pihak berwenang yang berhubungan. Tim keamanan juga harus dilatih secara teratur untuk memastikan bahwa mereka mampu merespons dengan cepat dan tepat terhadap insiden keamanan yang terjadi.

Selama proses penanganan kejadian keamanan, penting untuk memonitor dan mengevaluasi tindakan yang dilakukan untuk memastikan bahwa insiden keamanan telah diatasi dan tidak terjadi lagi di masa depan. Proses evaluasi ini juga harus mencakup analisis root cause dari insiden keamanan dan rekomendasi perbaikan sistem keamanan IT agar dapat mencegah terjadinya insiden serupa di masa depan.

Peningkatan sistem keamanan IT harus dilakukan secara terus-menerus berdasarkan hasil evaluasi tersebut, termasuk pembaruan dan perbaikan sistem keamanan, serta pelatihan dan pengembangan staf keamanan. Proses ini harus menjadi bagian dari siklus keamanan informasi organisasi untuk memastikan bahwa sistem keamanan tetap efektif dalam mengatasi ancaman keamanan yang terus berkembang (Rohman, 2020).

10.7.3 Memonitor dan mengevaluasi penanganan kejadian keamanan

Setelah insiden keamanan terjadi dan prosedur penanganan kejadian telah dilakukan, organisasi harus melakukan pemantauan dan evaluasi terhadap proses penanganan. Hal ini bertujuan untuk mengidentifikasi kesalahan atau kelemahan dalam prosedur penanganan kejadian yang dilakukan, serta untuk meningkatkan kinerja sistem keamanan secara keseluruhan. Pemantauan dan evaluasi dapat dilakukan dengan memeriksa laporan insiden keamanan, melakukan analisis forensik terhadap sistem, serta melakukan debriefing dengan staf yang terlibat dalam penanganan kejadian.

Hasil evaluasi harus digunakan untuk meningkatkan sistem keamanan IT secara keseluruhan. Organisasi harus memperbarui rencana pemulihan keamanan IT dan prosedur penanganan kejadian keamanan berdasarkan temuan dan rekomendasi yang diperoleh dari evaluasi tersebut. Selain itu, organisasi juga harus memperbarui teknologi keamanan jaringan dan sistem keamanan secara teratur untuk mengurangi risiko serangan keamanan di masa depan. Pelatihan dan edukasi terhadap pengguna dan staf tentang keamanan informasi juga harus terus dilakukan untuk memastikan bahwa semua orang memahami pentingnya keamanan informasi dan mampu menghindari serangan keamanan (Umar, 2019).

10.7.4 Meningkatkan sistem keamanan IT berdasarkan hasil evaluasi

Hasil evaluasi dari penanganan kejadian keamanan harus digunakan untuk meningkatkan sistem keamanan IT. Hal ini meliputi perbaikan pada rencana pemulihan keamanan IT dan prosedur penanganan kejadian keamanan yang ada, serta

pengembangan sistem keamanan baru yang lebih efektif. Selain itu, pelatihan keamanan dan kesadaran keamanan juga harus ditingkatkan untuk memastikan bahwa seluruh staf memahami pentingnya keamanan informasi dan dapat merespons dengan cepat terhadap kejadian keamanan.

Pengembangan sistem keamanan baru dan peningkatan kesadaran keamanan merupakan hal yang sangat penting untuk meningkatkan kinerja sistem keamanan secara keseluruhan. Selain itu, organisasi juga dapat memanfaatkan hasil evaluasi untuk mengidentifikasi kelemahan dalam infrastruktur IT mereka dan memperbaikinya. Salah satu cara yang dapat dilakukan adalah dengan melakukan penilaian risiko secara teratur untuk mengidentifikasi potensi ancaman keamanan dan mengambil langkah-langkah pencegahan yang tepat. Hal ini akan membantu organisasi untuk terus meningkatkan keamanan sistem IT mereka dan memastikan bahwa mereka dapat melindungi data dan informasi mereka dari serangan keamanan yang merugikan (ramadhani, 2020).

DAFTAR PUSTAKA

Hariyono, R. C. S. 2018. Audit Sistem Informasi Menggunakan Framework COBIT 4.1 Pada Website Universitas Peradaban. Smart Comp: Jurnalnya Orang Pintar Komputer, 7(1).

Khoironi, S. C. 2020. Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. Jurnal Studi Komunikasi Dan Media, 24(1), 37-56.

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. 2018. Analisis manajemen risiko keamanan data sistem informasi (Studi kasus: RSUD XYZ). Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 2(1), 282-287.

Muthoharoh, A., Waznah, U., Slamet, S., Rahmasari, K. S., & Nur, A. V. 2021. Communication, information, and education (CIE) on food safety issues in Kalimojosari Village, Pekalongan. Community Empowerment, 6(7), 1159-1162.

Misbah, M. 2017. Asesmen Maturitas Manajemen Risiko Perusahaan Pada Kontraktor Kecil Dan Menengah. Jurnal Teknik Mesin Mercu Buana, 6(2), 147-154.

Pardani, K. K., & Damayanthi, I. G. A. E. 2017. Pengaruh Pemanfaatan Teknologi, Partisipasi Pemakai, Manajemen Puncak Dan Kemampuan Pemakai Terhadap Efektivitas Sistem Informasi Akuntansi. E-Jurnal Akuntansi Universitas Udayana, 19(3), 2234-2261.

Ikhwan, A., & Hendri, R. 2020. Analisis Perencanaan Strategs Sistem Informasi Dan Teknologi Informasi Menggunakan Framework Ward Dan Peppard Studi Kasus: Fakultas Komputer Umitra Indonesia. Jurnal Teknologi dan Informatika (JEDA), 1(1).

Simarmata, J., Romindo, R., Putra, S. H., Prasetio, A., Siregar, M. N. H., Ardiana, D. P. Y., ... & Jamaludin, J. 2020. Teknologi Informasi dan Sistem Informasi Manajemen. Yayasan Kita Menulis.

Ishak, A. 2020. Identifikasi: Kriteria untuk Menilai Teknologi Pengolahan Air Limbah. Jurnal Sistem Teknik Industri, 22(2), 33-40.

Darwis, D., Solehah, N. Y., & Dartnono, D. 2021. Penerapan Framework Cobit 5 Untuk Audit Tata Kelola Keamanan Informasi Pada Kantor Wilayah Kementerian Agama Provinsi Lampung. TELEFORTECH: Journal of Telematics and Information Technology, 1(2), 38-45.

Ramadhani, N. D., Putra, W. H. N., & Herlambang, A. D. 2020. Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, 2548, 964X.

Setyoko, A. T., & Kristiningrum, E. 2019. Pengembangan desain sistem keamanan pangan menggunakan Hazard Analysis Critical Control Point (Haccp) pada ukm produsen nugget ikan. Jurnal Standardisasi, 21(1), 1-8.

Putri, A. H., Naryoso, A., & Rahardjo, T. 2022. PENGELOLAAN IDENTITAS DALAM RELASI ROMANTIK PENYANDANG DISABILITAS DAN NON DISABILITAS. Interaksi Online, 10(3), 583-594.

Ikhsan, R. F. 2019. PENGUKURAN TINGKAT KESELARASAN APLIKASI DEPLOYER TERHADAP PROSES BISNIS MENGGUNAKAN FRAMEWORK COBIT 5.0 (STUDI KASUS DI PT. TELKOM AKSES BANDUNG) (Doctoral dissertation, Program Sistem Informasi S1 Fakultas Teknik Universitas Widyatama).

Kusuma, I. G. N. A. 2021. PERANCANGAN SIMPLE STATELESS AUTENTIKASI DAN OTORISASI LAYANAN REST-API BERBASIS PROTOKOL HTTP. Jurnal Manajemen Informatika dan Sistem Informasi, 4(1), 78-87.

Halim, V. F. S., Pradana, F., & Bachtiar, F. A. 2019. Pengembangan Sistem untuk Memonitor Aktivitas Media Sosial Berbasis Web (Studi Kasus Media Sosial Twitter Calon Legislatif pada Pemilihan Legislatif 2019). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, 2548, 964X.

Munawar, Z., & Putri, N. I. 2020. Keamanan Jaringan Komputer Pada Era Big Data. J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa, 2(01), 14-20.

Yulianto, R., & Aprilyani, F. 2020. Sistem Keamanan Jaringan Komputer Menggunakan Metode NDLC Dengan Linux Zentyal Pada Instansi KEMENKO Maritim. Jurnal Teknik Informatika, 6(2), 79-86.

Palinggi, S., & Allolinggi, L. R. 2019. Analisa Deskriptif Industri Fintech di Indonesia: Regulasi dan Keamanan Jaringan dalam Perspektif Teknologi Digital. Ekonomi Dan Bisnis UPNVJ, 6(2), 177-192.

Bustami, A., & Bahri, S. 2020. Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review. Unistek, 7(2), 59-70.

Yulianto, S., Apriyadi, R. K., Aprilyanto, A., Winugroho, T., Ponangsera, I. S., & Wilopo, W. 2021. Histori bencana dan penanggulangannya di Indonesia ditinjau dari perspektif keamanan nasional. PENDIPA Journal of Science Education, 5(2), 180-187.

Supriyanto, A., Aknuranda, I., & Putra, W. H. N. 2019. Penyusunan Disaster Recovery Plan (DRP) berdasarkan Framework NIST SP 800-34 (Studi Kasus: Departemen Teknologi Informasi PT Pupuk Kalimantan Timur). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, 2548, 964X.

Rohman, A. F., Ambarwati, A., & Setiawan, E. 2020. Analisis Manajemen Risiko IT Dan Keamanan Aset Menggunakan Metode OCTAVE-S. INTECOMS: Journal of Information Technology and Computer Science, 3(2), 298-310.

Umar, R., Riadi, I., & Handoyo, E. 2019. Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). J. Sist. Inf. Bisnis, 9(1), 47.

Ramadhani, N. D., Putra, W. H. N., & Herlambang, A. D. 2020. Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN, 2548, 964X.

BAB 11
KEBERLANGSUNGAN PERENCANAAN BISNIS

Oleh Luluk Tri Harinie

11.1 Pendahuluan

Bisnis dapat mengalami masalah dengan tingkat kesulitan yang berbeda-beda. Suatu masalah dengan kondisi darurat atau suatu kejadian jika tidak dikelola dengan baik dapat meningkat menjadi bencana atau krisis. Selain menciptakan gangguan yang tidak direncanakan yang dapat menodai citra organisasi, kejadian yang ekstrim jika tidak dikelola dengan baik dapat mengakibatkan kerusakan fisik atau lingkungan secara signifikan. Hal ini dapat menyebabkan kecelakaan yang signifikan pada karyawan atau bahkan kematian. Sebagai contoh kebakaran, jika tidak ditangani dengan cepat dapat mengakibatkan konsekuensi yang serius. Makanya organisasi harus siap menghadapi kejadian sebelum terjadi untuk meminimalkan dampaknya jika terjadi. Apalagi potensi masalah pada teknologi (seperti serangan virus atau peretasan) dalam dunia maju dengan transasksi bisnis yang dilakukan serba langsung, persedian tepat waktu, dan rantai pasokan yang dinamis, maka jika kehilangan sistem komunikasi bisa menjadi lebih mahal daripada mengalami peristiwa kebakaran (Savage, 2002).

Disadari potensi masalah yang timbul seringkali diabaikan. Dan jika kejadian tersebut terjadi, barulah timbul kesadaran mempertahankan bisnis melalui perbaikan dengan konsep keberlangsungan perencanaan bisnis atau dikenal

dengan istilah BCP (*Business Continuity Planning*). BCP pun muncul sebagi respon terhadap kebutuhan untuk melindungi dan memperbaiki kegiatan akibat dampak penghasil nilai kristis dari suatu organisasi (Herbane, 2010). Konsep ini penting dan harus dimiliki sektor bisnis mengingat potensi masalah pasti akan selalu ada. BCP telah menghasilkan perbaikan proses di banyak bidang (Jemelian, 2004). Supaya BCP bekerja efektif, maka BCP sebaiknya mencakup berbagai macam masalah dan faktor yang sifatnya lebih luas. Misalnya jika kondisi bencana yang tidak memungkinkan untuk bekerja di lokasi yang normal, BCP harus menangani berbagai macam masalah yang berkaitan dengan logistik. Ditambah dengan adanya ketidakjelasan pada metode, proses, dan prosedur kerja yang ada saat ini mungkin tidak dapat dipindahkan ke lokasi yang baru dan hal ini lah yang harus ditangani sebagai bagian dari BCP. Jelasnya bahwa perlu untuk organisasi menyerap konsep BCP ke dalam budaya dan pemikiran organisasi, kemudian mengambil keputusan yang rasional dan terinformasi lengkap tentang sifat BCP yang disesuaikan dengan risiko yang teridentifikasi dan terkuantifikasi. Makanya BCP telah berkembang menjadi sebuah sistem yang terintegrasi untuk identifikasi, manajemen, pengawasan dan pengurangan risiko (Zsidisin, et al., 2005). Hal ini juga mengisyaratkan BCP haruslah seorang eksekutif, tingkat dewan Direksi. Karena manajemen senior seringkali bertanggung jawab atas manajemen risiko secara keseluruhan di suatu organisasi, mereka harus mempertimbangkan untuk memimpin dalam mendanai pelaksanaan BCP (Jemelian, 2004). Konsep BCP dapat mengingatkan bahwa 1) Meningkatkan ketergantungan pada proses komputerisasi dan sistem informasi dengan risiko yang signifikan dari berbagai masalah yang mungkin terjadi; 2) Kecuali jika sudah memiliki proses formal yang harus diikuti saat bencana terjadi, atau kemungkinan kekacauan dan

kebingungunan besar terjadi; 3) Pencadangan dan perbaikan yang telah ditetapkan sebelumnya akan jauh lebih efisien dan mungkin jauh lebih murah dari pada tindakan darurat yang bersifat sementara; dan 4) Biaya kegagalan bisnis kemungkinan besar akan jauh lebih tinggi daripada biaya langsung atas suatu kejadian (Savage, 2002).

11.2 Pemahaman Tahap Keberlangsungan Perencanaan Bisnis

Penekanan terbesar biasanya dilakukan organisasi pada kondisi-kondisi ”bencana besar” seperti banjir, gempa bumi, dan serangan teroris. Kondisi-kondisi seperti ini relatif jarang terjadi dan menghadirkan tantangan yang unik. Sementara bagi gangguan-gangguan sehari-hari penekanannya relatif tidak ada, seperti pelanggaran keamanan, masalah pasokan, dan masalah kerusakan peralatan. Padahal hal-hal kecil inilah yang dapat menghancurkan produktivitas dan membuat perusahaan berjuang demi bertahan hidup (D'Amico, 2007).

Demi meminimalkan gangguan dan mempertahankan tingkat pertumbuhan, perusahaan harus melakukan pendekatan terhadap keberlangsungan perencanaan bisnis dari sudut pandang yang sama sekali baru. Perlu pemikiran lebih tentang tahap keberlangsungan dan tingkat gangguan. Ada tiga tahap dalam keberlangsungan perencanaan bisnis yang sistematis (D'Amico, 2007), yaitu tahap menangani, tahap menanggapi, dan tahap membangun kembali. Ketiga tahap tersebut disajikan pada tabel 11.1 berikut.

Tabel 11.1. Tiga Tahap Keberlangsungan

Menangani	Menanggapi	Membangun kembali
Mengidentifikasi peran dan tanggung jawab	Bereaksi dengan cepat	Menilai kerusakan
Mendokumentasikan proses-proses penting dalam misi	Melibatkan layanan tanggap darurat publik	Mengelola proses klaim asuransi
Membuat katalog aset-aset penting	Beritahukan kepada penanggap internal dan kontak utama lainnya	Libatkan sumber daya eksternal
Tentukan kontak utama	Ambil langkah-langkah untuk meminimalkan dan mengatasi kerusakan	Bawa peralatan cadangan secara langsung
Mengevaluasi risiko	Menstabilkan situasi	Mengkomunikasikan situasi dan rencana
Mengambil tindakan pencegahan	Menahan dampaknya	Mempercepat kembalinya ke keadaan normal

Sumber: (D'Amico, 2007)

Pendekatan perusahaan biasanya tidak akan berhasil jika dilakukan dengan menulis secara manual terkait tanggap bencana yang mencakup semua tahap dan gangguan. Dan hal ini menghasilkan waktu yang hilang, pendapatan yang hilang, dan peluang yang hilang. Makanya perlu adanya panduan untuk menjaga perusahaan tetap berada di jalur pertumbuhan dan terhindar dari kebangkrutan saat terjadi peristiwa yang tidak bisa terhindarkan terjadi. Berikut penjelasan ketiga tahap keberlangsungan perencanaan bisnis (D'Amico, 2007).

1. Tahap Menangani
   Tahap menangani merupakan tahap mengambil keputusan untuk menghadapi potensi bencana dan mengambil tindakan untuk mencegahnya. Berikut adalah beberapa pertanyaan kunci yang perlu dijawab dalam upaya ini, antara lain:
   1) Siapa saja yang perlu dilibatkan dalam mengembangkan perencanaan pemulihan bencana?
   2) Apa saja proses bisnis yang penting bagi organisasi dan peralatan pendukungnya?

3) Berapa lama masing-masing proses tersebut tidak tersedia tanpa melumpuhkan perusahaan?
4) Apa saja pilihan untuk mengganti atau mengalihdayakan proses-proses tersebut dalam keadaan darurat?
5) Pemasok, mitra, dan perusahaan luar mana saja yang dapat merespons dengan cepat?
6) Risiko apa yang dihadapi organisasi?
7) Langkah-langkah apa yang dapat diambil untuk mengurangi risiko?

Setelah menjawab pertanyaan-pertanyaan tersebut, ada kecenderungan untuk langsung mendokumenkan prosedur tanggap darurat. Namun saat ini lebih baik menginvestasikan pengelolaan proses bisnis dan risiko organisasi. Saat ini perlu untuk mendokumenkan kondisi dan sediakan prosedur untuk tindakan pencegahan yang sedang berlangsung untuk mengurangi risiko.
Setiap bisnis yang berkembang, proses akan berubah, orang akan datang dan pergi, peralatan akan diganti, dan produk akan berkembang. Saat perubahan ini terjadi, risiko akan berkembang dan berpindah. Menerapkan prosedur untuk memantau, mendokumenkan, dan memelihara lingkungan secara memadai. Misalnya kelompok fasilitas harus memiliki prosedur tertulis untuk kegiatan pemeliharaan rutin di dalam dan di luar gedung. Hal ini harus mencakup langkah-langkah untuk mencegah kerusakan akibat air dan kebakaran serta inspeksi listrik secara rutin. Demikian juga pada kelompok TI harus memiliki prosedur pencadangan yang terdokumen dengan jelas, prosedur pemeliharaan jaringan secara teratur, dan pemeriksaan keamanan yang konstan.

Memiliki dokumen yang ditargetkan untuk memandu setiap departemen dalam mencegah bencana akan menghindari banyak kejadian saat kondisi darurat yang umum terjadi seperti kebakaran kecil, kerusakan air, atau pelanggaran keamanan. Ketika bencana terjadi, kemungkinan besar akan lebih kecil dan lebih mudah ditangani daripada jika tindakan pencegahan tidak dilakukan.

Daftar periksa merupakan alat yang sangat baik untuk mengingatkan orang-orang tentang apa yang perlu dilakukan dan memandu mereka melalui serangkaian langkah. Daftar periksa juga mudah ditandatangani dan disimpan sebagai verifikasi bahwa pekerjaan telah dilakukan. Buatlah daftar periksa satu halaman yang sederhana untuk semua kegiatan-kegiatan pencegahan bencana.

Setelah langkah-langkah untuk mencegah terjadinya bencana telah tersedia, saatnya untuk mengalihkan perhatian organisasi pada apa yang harus dilakukan. Perhatian organisasi pada apa yang harus dilakukan jika bencana terjadi, meskipun sudah ada upaya-upaya tersebut. Ini adalah upaya perencanaan tanggap darurat.

2. Tahap Menanggapi

   Tahap menanggapi merupakan tahap terberat dari ketiga tahap tersebut. Mungkin akan terjadi kekacauan selama kondisi tanggap darurat. Para penanggap harus tahu apa yang harus dilakukan sebelumnya atau mereka akan hancur, karena beratnya peristiwa. Berikut adalah beberapa kunci yang perlu dijawab selama perencanaan tanggap darurat, antara lain:

   1) Siapa saja yang perlu diikutsertakan dalam tim tanggap bencana?
   2) Siapa yang akan menyatakan bencana?
   3) Bagaimana tim tanggap bencana akan berkomunikasi?

4) Bagaimana informasi akan disebarkan kepada semua karyawan?
5) Bagaimana polisi, pemadam kebakaran, dan petugas darurat lainnya akan dilibatkan?
6) Di mana orang-orang akan beroperasi dan dengan peralatan apa?
7) Bagaimana pelanggan, pemasok, mitra, dan pihak lain akan diberitahu, jika perlu?

Salah satu hal yang membuat perencanaan bencana menjadi rumit adalah beragamnya kondisi yang harus ditangani. Sebuah bencana bisa saja sesederhana seperti kebakaran kecil yang memicu sprinkler yang menyebabkan sebagian besar kerusakan air. Bencana juga bisa menjadi bencana besar seperti kecelakaan besar atau kecelakaan industri yang mengakibatkan kehancuran total sebuah fasilitas beserta korban jiwa.

Jangan memperlakukan tahap ini sebagai ''satu ukuran untuk semua''. Mulailah dengan mendokumenkan respons dasar, orang-orang yang akan dilibatkan dan informasi kontak untuk semua orang yang mungkin perlu diberitahu. Hal ini akan menjadi dasar yang baik dapat dipahami dan diterima oleh semua orang.

Seringkali masalah terbesar selama krisis adalah kesulitan komunikasi. Buatlah daftar kontak. Simpanlah di berbagai lokasi dengan menggunakan berbagai format, baik elektronik maupun cetak. Perencanaan kebutuhan lebih dari satu mekanisme media komunikasi. Pertimbangkan untuk menggunakan telepon rumah, telepon genggam, pager, e-mail, pesan instan, dan telepon satelit. Beberapa dari media komunikasi ini mungkin tidak akan tersedia saat terjadi bencana besar.

Lanjutkan dengan mendokumenkan prosedur untuk menyiapkan peralatan pengganti di dalam fasilitas-fasilitas

yang ada saat ini atau di dekatnya. Jangan membuat kesalahan dengan mengasumsikan bahwa karena data cadangan disimpan di luar lokasi, tidak ada yang perlu dikhawatirkan. Jika peralatan rusak atau fasilitas tidak dapat digunakan, maka data cadangan tidak akan berguna.

Keuntungan utama dari pendekatan ini bahwa dokumen untuk menangani kondisi yang paling umum akan menjadi singkat dan tepat sasaran. Penanggap pertama akan mengetahui dengan pasti apa yang mereka harus lakukan dalam menangani keadaan darurat yang paling mungkin terjadi.

Penting untuk mengendalikan kondisi darurat kecil dengan cepat, sehingga tidak memiliki kesempatan untuk menjadi bencana besar. Jika terjadi bencana besar, perencanaan tersebut harus melibatkan orang-orang tambahan di dalam dan di luar organisasi. Manajer yang lebih senior juga perlu dilibatkan untuk membantu mengelola upaya tersebut. Setelah kondisi darurat segera stabil, perhatian beralih ke pembangunan kembali dan kondisi kembali normal.

3. Tahap Membangun Kembali

   Tahap membangun kembali secara sederhana dapat mengganti peralatan yang rusak atau secara rumit dengan merekonstruksi seluruh fasilitas dan isinya. Berikut adalah beberapa pertanyaan kunci yang perlu dijawab selama perencanaan pembangunan kembali, antara lain:

   1) Siapa yang perlu dilibatkan dalam upaya pembangunan kembali?
   2) Siapa yang akan bertanggung jawab atas penilaian kerusakan?
   3) Bagaimana klaim asuransi akan ditangani?
   4) Apa yang akan dilakukan untuk mempertahankan tingkat produktivitas?

5) Penyesuaian apa yang akan dilakukan dalam kondisi kerja dan jam operasi?

Tahap ini dipengaruhi oleh sejumlah kriteria. Misalnya: Apakah fasilitas tersebut dimiliki atau disewa? Apakah fasilitas tersebut sepenuhnya ditempati atau digunakan bersama? Apakah peralatan dimiliki atau disewa? Apakah mesin tersedia di pasaran atau dirancang khusus?

Jawaban atas pertanyaan-pertanyaan ini dan banyak pertanyaan terkait lainnya perlu didokumenkan. Kontak utama harus diidentifikasi. Dalam situasi pasca bencana banyak pemasok yang siap dan bersedia membantu, namun waktu adalah hal yang penting. Perlu untuk melibatkan mereka sesegera mungkin.

Tingkat kerusakan yang terjadi harus dinilai tidak hanya untuk tujuan asuransi, namun juga karena barang dengan waktu tunggu yang lama harus dipesan sesegera mungkin untuk meminimalkan waktu henti. Di sinilah perlu untuk mendokumenkan dengan baik bagi semua aset perusahaan menjadi sangat berharga. Hal ini akan menyederhanakan klaim asuransi dan pemesanan penggantian.

Idealnya tahap menanggapi dan tahap membangun kembali akan sedikit tumpang tindih, sehingga waktu perbaikan dapat dipersingkat. Memiliki orang dan mendokumenkan secara terpisah sebagai upaya menyederhanakan dan mempercepat kedua upaya tersebut.

11.3 Pemahaman Proses Keberlangsungan Perencanaan Bisnis

Selanjutnya perencanaan yang dihasilkan BCP memang penting, maka perlu untuk dipahami tentang proses pembuatan perencanaan tersebut. Pemikiran yang serius tentang bisnis dan kemungkinan efek dari berbagai kejadian darurat perlu dilakukan. Proses ini menghasilkan perencanaan dengan

melibatkan berbagai kegiatan (Savage, 2002) seperti: 1) Dampak bisnis dan analisis risiko; 2) Mendokumenkan kegiatan yang diperlukan untuk mempersiapkan organisasi dalam menghadapi kemungkinan darurat (termasuk langkah-langkah pemulihan strategis); 3) Mengidentifikasi dan mengesahkan rincian kegiatan terperinci untuk setiap tahap pemulihan bencana; 4) Mengidentifikasi dan mengesahkan kegiatan terperinci untuk mengelola proses pemulihan bisnis; 5) Menguji dan mengaudit proses pemulihan bisnis; 6) Melatih staf dalam proses pemulihan bisnis; dan 7) Menerapkan proses untuk menjaga supaya rencana-rencana pemulihan bisnis yang terbaru.

Saat melakukan proses kegiatan BCP ini, akan sangat berguna mengumpulkan dokumen yang diperlukan sebagai bagian dari proses. Dokumen tersebut (Savage, 2002) mencakup: 1) Bagan organisasi yang menunjukkan nama dan posisi, dan terutama mereka yang memiliki wewenang khusus untuk bertindak dalam situasi darurat; 2) Informasi kontak darurat untuk staf khusus (dan terutama mereka yang merupakan bagian integral dari proses pemulihan bisnis); 3) Nomor kontak untuk layanan darurat; 4) Nomor kontak untuk pemasok yang mungkin diperlukan untuk berkontribusi pada proses pemulihan bisnis; 5) Informasi kontak darurat untuk setiap penasihat/konsultan profesional; 6) Peta dan denah semua lokasi, spesifikasi dari semua sistem TI dan komunikasi utama, dan khususnya rincian proses pencadangan dan pemulihan; 7) Salinan perjanjian pemeliharaan/layanan; 8) Perjanjian tingkat layanan; 9) Prosedur evakuasi dan peraturan kebakaran, prosedur kesehatan dan keselamatan; 10) Prosedur operasi dan administrasi standar; 11) Inventaris aset; 12) Rincian penyimpanan di luar lokasi; 13) Peraturan dan pedoman industri yang relevan; dan 14) Informasi asuransi.

11.3.1 Dampak Bisnis dan Analisis Risiko

Proses keberlanjutan perencanaan bisnis salah satunya dengan mempertimbangkan dampak potensial dari setiap jenis masalah atau bencana atau kejadian darurat yang mungkin terjadi (Savage, 2002). Pada tingkat dasar, analisis dampak bisnis adalah cara untuk menilai secara sistematis dampak potensial yang terjadi dari berbagai peristiwa atau insiden yang mungkin menyebabkan sistem atau fasilitas yang ada di organisasi tidak tersedia. Seringkali dampak dari jenis insiden (non-darurat) lainnya (seperti pelanggaran kerahasiaan atau hilangnya integritas data) dieksplorasi pada saat yang sama untuk masalah atau kejadian yang baru muncul demi menetapkan BCP yang komprehensif.

Analisis dampak bisnis membantu organisasi untuk memahami tingkat potensi kerugian (dan efek yang tidak diinginkan lainnya) yang dapat terjadi. Kerugian tersebut tidak hanya mencakup kerugian finansial secara langsung, tetapi juga kerugian potensial dan konsekuensial lainnya, seperti hilangnya kepercayaan pelanggan, rusaknya reputasi, dll.

Cara sederhana untuk memeriksa dampak tersebut adalah dengan mengidentifikasi proses bisnis utama dan kemudian memeriksa dampak dari skenario darurat/bencana yang mungkin terjadi pada masing-masing proses bisnis tersebut. Proses-proses bisnis utama tersebut dapat meliputi: proses produksi, proses pasokan, proses pergudangan dan distribusi, proses jaminan dan kontrol kualitas, proses penjualan dan administrasi penjualan, proses hubungan dengan pelanggan, proses pemeliharaan dan perbaikan, proses sistem informasi, proses komunikasi (telepon, email, faks, dll.), proses keuangan, proses penelitian dan pengembangan, proses manajemen sumber daya manusia, dan proses pendukung bisnis (tempat, katering, kebersihan, dll.). Selanjutnya cara yang dimungkinkan untuk menganalisis dan mengevaluasi

dampak adalah dengan menetapkan batas waktu standar sebagai dasar evaluasi. Misalnya dampak terhadap bisnis dapat dinilai jika layanan atau proses tertentu tidak tersedia selama 2 jam, 2-24 jam, 1 hari, dll.

Sejalan dengan penilaian dampak, penting untuk mempertimbangkan tingkat risiko yang terkait dengan peristiwa apa pun yang terjadi. Menganalisis risiko digunakan untuk menentukan kondisi kejadian/bencana mana yang harus diperhatikan lebih besar selama menyusun BCP.

1. Analisis Risiko Kuantitatif
   Pendekatan ini umumnya menggunakan dua komponen, yaitu probabilitas terjadinya suatu peristiwa dan kemungkinan terjadinya kerugian jika terjadi. Kedua hal ini digabungkan (dengan perkalian) untuk menghasilkan satu angka. Hal ini terkadang dikuantifikasi sebagai ekspektasi kerugian tahunan (*annual loss expectancy*/ ALE) atau estimasi biaya tahunan (*estimated annual cost*/EAC). Kemudian dimungkinkan untuk mengurutkan kejadian-kejadian dalam urutan risiko berdasarkan ALE dan pada akhirnya membuat keputusan berdasarkan hal ini.
   Masalah dengan analisis kuantitatif seperti itu mengisyaratkan "ketepatan". Seringkali data yang digunakan dalam menyusun ALE tidak tepat atau hanya perkiraan. Oleh karena itu, angka-angka yang dihasilkan harus digunakan dengan hati-hati.
2. Analisis Risiko Kualitatif
   Pada analisis ini data probabilitas tidak diperlukan dan hanya estimasi potensi kerugian yang digunakan. Banyak metode analisis risiko kualitatif yang menggunakan sejumlah elemen yang saling terkait, seperti:
   1) Ancaman. Hal ini dapat menjadi salah satu yang "membahayakan" sistem. Contohnya seperti kebakaran

atau penipuan. Ancaman selalu ada pada setiap sistem dalam organisasi.

2) Kerentanan. Hal ini merupakan faktor-faktor yang membuat sistem lebih rentan terhadap serangan ancaman atau membuat serangan lebih mungkin berhasil atau berdampak. Misalnya, keberadaan bahan yang mudah terbakar di lokasi tertentu meningkatkan kerentanan terhadap ancaman kebakaran.
3) Pengawasan. Hal ini merupakan kebalikan dari kerentanan dan terdiri dari empat tipe dasar, yaitu pengawasan sebagai pencegah untuk mengurangi kemungkinan serangan yang disengaja, pengawasan pencegahan yang melindungi kerentanan dan "menetralisir" potensi insiden atau mengurangi dampaknya, pengawasan perbaikan yang mengurangi dampak dari suatu insiden; dan pengawasan deteksi yang menemukan insiden dan memicu pengawasan pencegahan atau perbaikan.

11.3.2 Masalah Bangunan.

Jika kondisi darurat memengaruhi bangunan organisasi, maka perlu untuk dapat bergerak cepat dalam melakukan perbaikan atau tindakan darurat. Strategi yang mungkin dilakukan untuk mengatasi bencana besar antara lain:

1. Memiliki akses ke fasilitas kosong yang dapat segera digunakan. Hal ini biasanya terlalu mahal untuk dapat dilakukan secara ekonomis.
2. Mengidentifikasi bangunan yang ada di mana kegiatan atau layanan yang tidak penting dapat dipindahkan dan digantikan oleh kegiatan atau layanan yang penting, jika bangunan utama terkena dampak.

3. Menetapkan pengaturan siaga dengan penyedia layanan kantor untuk menyediakan layanan yang sesuai dalam jangka waktu yang disepakati.

Tentu saja dalam banyak kasus, pemindahan (relokasi) menyeluruh seperti itu tidak diperlukan. Masalahnya hanya untuk mengatasi gangguan, sementara perbaikan dilakukan pada bangunan yang terkena dampak. Maka penting untuk mengidentifikasi dalam keberlangsungan perencanaan bisnis bagi beberapa orang yang memiliki wewenang dan tanggung jawab untuk memulai tindakan (berbiaya mahal).

Bangunan saat ini mungkin disewa atau disewakan, pemilik atau penyewa mungkin bertanggung jawab untuk hal ini dalam mengambil tindakan. Kewenangan dan tingkat kewenangan tersebut harus diketahui atau ditetapkan terlebih dahulu jika tindakan harus diambil dengan cepat. Misalnya individu atau tim yang bertanggung jawab untuk memulihkan tempat supaya dapat berfungsi normal, harus mengetahui tingkat kewenangan untuk menugaskan pekerjaan bagi agen dan kontraktor eksternal. Dalam kondisi darurat yang nyata, sulit untuk mendapatkan persetujuan dari kondisi mendesak untuk pekerjaan tersebut. Makanya keberlanjutan perencanaan bisnis harus berisi informasi tentang tingkat kewenangan yang berlaku dan langkah-langkah yang diperlukan untuk memperpanjangnya.

Dalam perencanaan tersebut juga berisi daftar semua bangunan yang dimiliki atau digunakan oleh organisasi beserta rinciannya. Mencakup: 1) Apakah itu hak milik, hak guna bangunan, atau sewa; 2) Tanggung jawab untuk perbaikan dan pemeliharaan bahan, perlengkapan dan perabotan; 3) Perlindungan asuransi; 4) Persetujuan eksternal (misalnya peraturan bangunan atau perencanaan, kontrol apa pun yang terkait dengan status "terdaftar", dll.) yang diperlukan sebelum

pekerjaan dapat dimulai; 5) Tingkat kewenangan internal dan rincian persetujuan yang diperlukan sebelum menugaskan kontraktor; 6) Prosedur untuk memperpanjang persetujuan dalam situasi darurat; dan 7) Orang yang bertanggung jawab atas kegiatan pemulihan lokasi, bersama dengan rincian kontak daruratnya.

Perhatian khusus diberikan pada layanan terutama listrik. Keberlanjutan perencanaan harus mencakup penyediaan generator cadangan atau catu daya yang dapat dipadamkan untuk memungkinkan proses bisnis yang terpenting dapat tetap dilanjutkan, atau dapat ditutup ketika terjadi pemadaman listrik. Hal ini terutama berlaku untuk sistem TI di mana data dapat rusak akibat pasokan listrik yang terputus-putus dan bahkan ada potensi lonjakan atau penurunan daya saat listrik mati, maka generator cadangan dapat dinyalakan.

Keberlangsungan perencanaan bisnis harus mendokumenkan keberadaan generator cadangan *dan uninterruptible power supply* (UPS) serta fungsi-fungsi yang dapat mendukung atau mengelola organisasi. Rencana tersebut juga harus merinci prosedur pengujian dan mencatat kapan terakhir kali diuji.

11.3.3 Masalah IT

Seperti yang telah disebutkan sebelumnya, banyak orang yang menyamakan BCP dengan perencanaan perbaikan kerusakan TI. Tentu saja sistem TI yang tersebar luas membuat masalah TI menjadi komponen penting dalam BCP. Keberlanjutan perencanaan bisnis harus berisi spesifikasi rinci dari sistem TI utama dan infrastruktur jaringan lokal dan jaringan area luas yang mendukung. Bagi organisasi yang lebih besar dengan sistem TI berskala besar dan kompleks, mungkin lebih tepat untuk menempatkan spesifikasi ini dalam lampiran

pada dokumen utama. Dokumen tersebut harus memperjelas proses bisnis utama dan kegiatan fungsional yang bergantung pada masing-masing sistem.

Karena perubahan TI cukup sering dan cukup cepat, maka penting untuk selalu memperbarui spesifikasi dan konfigurasi sistem saat sistem ditingkatkan atau dimodifikasi. Sehingga BCP merupakan kegiatan yang berkelanjutan dan merupakan bagian dari sistem pengawasan perubahan TI secara formal.

Prosedur pencadangan dan perbaikan TI yang sudah ada dan normal harus didokumenkan dalam keberlangsungan perencanaan bisnis bersama dengan rincian pengaturan penyimpanan data/media di luar lokasi. Untuk setiap proses/kegiatan/sistem utama, perlu ditentukan jenis proses pencadangan yang sesuai. Pada tingkat yang berbeda untuk proses administratif yang sederhana, mungkin cukup untuk mencadangkan proses komputerisasi dengan proses manual (mungkin didukung oleh PC yang berdiri sendiri). Tentu saja sifat proses perbaikan akan menentukan kecepatannya. Kecepatan perbaikan yang direncanakan ini harus sesuai dengan penelitian dampak yang dinilai berdasarkan rentang waktu yang dilakukan sebelumnya.

Sistem TI mungkin perlu diperbaiki/dipulihkan jika terjadi kejadian terkait TI atau yang lebih umum yang berbasis bangunan. Kejadian berbasis bangunan yang signifikan (pemadaman listrik, kebakaran, banjir, dll.) hampir pasti akan berdampak pada infrastruktur TI yang mendasarinya atau sistem utama itu sendiri.

Mungkin akan lebih baik jika memiliki alternatif-alternatif yang tersedia untuk sistem-sistem utama dalam keadaan darurat. Idealnya hal ini hanya melibatkan pengalihan otomatis ke bangunan alternatif atau paling banyak transfer media data utama ke bangunan alternatif, agar sistem dapat

diaktifkan kembali dan tersedia untuk bisnis. Tentu saja fasilitas alternatif yang siap pakai seperti itu mungkin sangat mahal, namun dengan meningkatnya penggunaan *outsourcing*, penyediaan layanan terkelola, dan penyediaan layanan aplikasi (*application service provision*/ASP), fasilitas untuk mendukung pilihan tersebut sering kali tersedia.

11.3.4 Masalah Layanan Pelanggan

Sangat penting bagi organisasi untuk terus memberikan tingkat layanan yang memadai kepada pelanggannya selama kondisi darurat atau menginformasikan kepada pelanggan (dan calon pelanggan) tentang alasan kegagalan pengiriman barang atau jasa. Layanan dan proses utama yang berhubungan dengan pelanggan harus dirinci dalam kelangsungan perencanaan bisnis bersama dengan indikasi prioritasnya. Untuk kegiatan/proses prioritas tinggi, harus ada indikasi strategi yang harus diikuti jika terjadi gangguan. Semua pelanggan yang terkena dampak harus diberitahu tentang potensi gangguan pada layanan sesegera mungkin.

11.3.5 Masalah Teknis Operasional Administrasi

Tugas-tugas "*back office*" harus diprioritaskan menjadi penting/tidak penting, dan waktu yang tidak kritis selama periode waktu tertentu (mungkin menggunakan rentang waktu yang sama dengan yang digunakan sebelumnya). Ketika bencana bergerak dari jangka pendek ke jangka panjang, karena waktu yang dibutuhkan untuk memulihkan fungsi-fungsi penting dengan lebih banyak kegiatan akan bergerak dari 'kurang' menjadi 'lebih' penting.

Metode alternatif untuk menangani setiap tugas ini harus diidentifikasi. Beberapa di antaranya hanya akan menggantikan proses otomatis dan terkomputerisasi dengan proses manual. Strategi perbaikan perlu ditentukan bagi

informasi dan dokumen penting demi menetapkan tingkat dasar kegiatan administratif meskipun gangguan mungkin terjadi membuat akses ke sumber informasi penting menjadi sulit. Makanya bagian dari perencanaan ini juga akan berisi rincian sumber informasi utama, data dan dokumen yang digunakan oleh organisasi serta rincian ketersediaan cadangan atau keberadaan sumber-sumber alternatif.

11.3.6 Masalah Pertanggungan Asuransi

Beberapa perusahaan asuransi umum dan sejumlah kecil pialang asuransi khusus, akan menangani asuransi untuk kondisi darurat. Perlindungan asuransi harus dipertimbangkan untuk bangunan utama dan bangunan lainnya, serta untuk biaya yang dikeluarkan dalam menangani kondisi darurat. Pertimbangan yang juga harus diberikan pada asuransi komersial terhadap, misalnya klaim non-kinerja atau pelanggaran kontrak oleh pelanggan dan klien, potensi kerugian konsekuensial lainnya dan untuk kehilangan pendapatan perdagangan. Masalah yang lebih sensitif dan penting adalah asuransi terhadap kehilangan karyawan inti.

Keberlangsungan perencanaan bisnis harus mencantumkan semua polis asuransi yang sesuai, sifat, jumlah dan jangka waktu pertanggungan, orang yang bertanggung jawab untuk mempertahankan pertanggungan yang memadai, tanggal perpanjangan berikutnya, rincian kontak, dll.

11.3.7 Masalah Kepegawaian

Komponen utama dalam BCP adalah penetapan strategi penanganan tenaga kerja. Ini adalah masalah yang sensitif, dimana perencanaan tersebut harus menyeimbangkan kebutuhan organisasi untuk mempertahankan tingkat kepegawaian yang memadai dan sesuai dengan potensi kepekaan staf dan keluarganya (jika terdampak).

Daftar staf yang terbaru harus disertakan dalam perencanaan tersebut. Daftar ini harus mencakup rincian kontak standar dan darurat untuk semua karyawan. Sebagai bagian dari proses penanganan darurat dan bukan keberlanjutan perencanaan bisnis. Harus ada prosedur untuk memperhitungkan keselamatan semua anggota staf.

Jika kejadian terjadi di luar jam kerja normal, mungkin perlu menghubungi staf untuk menginformasikan kejadian tersebut dan memberikan instruksi tentang cara untuk tetap berhubungan dengan kejadian selama proses pemulihan. Pilihan di sini termasuk pesan yang telah direkam sebelumnya yang ditinggalkan di nomor telepon khusus atau situs web darurat.

11.3.8 Dokumen

Penyimpanan dokumen penting, tidak mengherankan termasuk dalam keberlanjutan perencanaan bisnis itu sendiri. Perencanaan ini harus dapat bertahan dari kejadian besar apa pun, termasuk kebakaran. Beberapa bentuk penyimpanan di luar lokasi (salinan) terhadap dokumen-dokumen penting tersebut harus dipertimbangkan. Untuk organisasi dengan banyak lokasi, bisa menyimpan salinan dokumen-dokumen penting di lebih dari satu lokasi dan tentu saja memiliki perubahan prosedur pengawasan demi memastikan bahwa setiap salinan telah direvisi saat dokumen diperbarui. Penyimpanan di luar lokasi yang terlindungi dan komersial juga tersedia di sebagian besar kota besar.

Makanya keberlangsungan perencanaan bisnis harus berisi rincian semua lokasi penyimpanan tersebut termasuk alamat lengkap, kontak dan rincian akses, termasuk siapa yang memiliki wewenang untuk mengaksesnya. Hal ini harus mencakup rincian tentang cara mengakses dokumen tersebut dengan cepat dalam keadaan darurat. Bagian dari perencanaan

ini juga harus mencakup rincian personil yang bertanggung jawab atas penyimpanan dan pembaruan catatan atau data tersebut.

Sebagai bagian dari persiapan untuk suatu kejadian, mungkin perlu untuk memastikan pasokan alat tulis yang telah dicetak sebelumnya dan perlengkapan kantor lainnya, yang mungkin hilang atau rusak. Hal ini mungkin melibatkan penyimpanan stok darurat (sekali lagi, sebaiknya di luar lokasi, lokasi yang aman) atau cukup dengan memelihara daftar pemasok peralatan tulis yang dapat dihubungi dengan segera dalam keadaan darurat.

11.3.9 Menangani Media

Saat kondisi darurat apa pun, pers dan TV kemungkinan besar akan mengajukan pertanyaan. Bagi kondisi darurat yang besar, kemungkinan menjadi berita televisi nasional dan bagi kondisi darurat yang lebih kecil kemungkinan hanya pers lokal. Namun apa yang diberitakan dapat berdampak pada bisnis melalui perubahan ekspektasi pelanggan (dan calon pelanggan), karyawan, dan pemangku kepentingan lainnya. Keberlanjutan perencanaan bisnis harus menjelaskan siapa yang bertanggung jawab untuk menangani pertanyaan dari media dan siapa yang bertanggung jawab untuk mengeluarkan pernyataan pers yang proaktif, jika diperlukan.

11.3.10 Biaya

Setiap komponen atau fase dari perencanaan tersebut akan menimbulkan biaya jika harus dilaksanakan. Tentu saja beberapa biaya dapat ditutup melalui klaim asuransi, tetapi kemungkinan besar pengeluaran akan diperlukan sebelum klaim tersebut diproses. Pengeluaran ini harus disetujui terlebih dahulu, karena wewenang tersebut mungkin tidak tersedia dalam keadaan darurat.

11.3.11 Menguji, Mengaudit, Dan Terus Mengikuti Perkembangan

Setelah mengembangkan rencana, sangat masuk akal untuk mengujinya dan kemudian melakukan audit secara berkala. Menjaga agar rencana keberlanjutan bisnis tetap mutakhir itu sulit. Sering kali perencanaan dibuat dengan penuh semangat dan perhatian, namun kemudian ditinggalkan begitu saja. Proses pengujian dan audit membantu memastikan bahwa perencanaan tersebut tetap mutakhir dan dapat bertahan dalam pemeriksaan ketat. Pengujian memang sulit dilakukan, karena tidak mungkin dilakukan dalam kondisi yang sangat tertekan dalam keadaan darurat yang sesungguhnya. Tetapi sebuah simulasi atau bahkan sebuah penelusuran sederhana terhadap rencana tersebut, dapat mengungkap ketidakkonsistenan atau kelalaian.

Pendekatan untuk menguji/audit meliputi: penggunaan konsultan spesialis, bekerja dengan menggunakan format dan daftar periksa, penggunaan tim uji/audit internal dengan beberapa pelatihan khusus, dan tukar pikiran secara sederhana tentang rencana tersebut oleh karyawan kunci melalui pertemuan dan lokakarya intensif. Pengendalian perubahan formal harus digunakan untuk mengelola perubahan pada perencanaan.

DAFTAR PUSTAKA

Chen, S. & Xu, J., 2022. COVID-19, business continuity management and standardization: case study of Huawei. *Chinese Management Studies,* 23 August.pp. 1-22.

D'Amico, V., 2007. Master the three phases of business continuity planning. *BUSINESS STRATEGY SERIES,* 8(3), pp. 214-220.

Herbane, B., 2010. Small business research: time for a crisis-based view. *International Small Business Journal,* 2(8), pp. 43-64.

Jemelian, B., 2004. Business continuity planning. *THE JOURNAL OF RISK FINANCE,* 5(4), pp. 29-31.

Savage, M., 2002. Business Continuity Planning. *Work Study,* 51(5), pp. 254-261.

Zsidisin, G. A., Melnyk, S. A. & Ragatz, G. L., 2005. An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research,* 43(16), pp. 3401-3420.

BAB 12
JAMINAN KUALITAS DAN STANDAR ASQ

Oleh Wirawan Istiono

12.1 Apakah Standar Kualitas itu?

Patokan mutu dicirikan sebagai arsip yang memberikan persyaratan, ketetapan, aturan, atau ciri-ciri yang dapat dimanfaatkan secara andal untuk menjamin bahwa bahan, barang, bentuk, dan administrasi sesuai dengan fungsinya. Panduan memberi organisasi visi, pemahaman, strategi, dan leksikon bersama yang diperlukan untuk memenuhi keinginan mitra mereka. Karena tindakan menunjukkan penggambaran dan ungkapan yang tepat, mereka menawarkan premis yang objektif dan pasti bagi organisasi dan pelanggan di seluruh dunia untuk berkomunikasi dan melakukan perdagangan (Asq.org, 2022).

Tahap penting dalam proses manajemen kualitas adalah jaminan kualitas. Kualitas produk, yang dapat dicapai dengan menggunakan ukuran standar kualitas, menentukan nilai pasarnya. Kepuasan pelanggan, yang dapat dicapai dengan menerapkan standar kualitas, juga menjadi faktor kualitas produk. Saat ini, mencapai kualitas sangat penting karena meningkatnya harapan klien. Standar harus diikuti untuk sertifikasi kualitas sektor TI dan bisnis. Organisasi bisnis dapat meningkatkan nilainya di pasar global dengan menerapkan standar (Manghani, 2011).

Organisasi Internasional untuk Standardisasi (ISO) mengembangkan standar mutu ISO 9000:2000, yang

melibatkan peningkatan keterlibatan manajemen puncak dan perbaikan berkelanjutan. Model Kualitas untuk produk perangkat lunak disarankan oleh beberapa standar yang diusulkan secara luas, termasuk ISO/IEC (International Electro technical Commission) 9126 dan ISO/IEC 25000.

Gambar 12.1. Prinsip Standar Kualitas
(Sumber : asq.org)

12.2 Siapa yang Menggunakan Standar Kualitas

Organisasi melihat standar kebijakan, definisi, dan prosedur untuk membantu mencapai tujuan seperti:

- Memenuhi persyaratan kualitas pelanggan
- Memastikan keamanan produk dan layanan
- Mematuhi peraturan
- Mencapai tujuan lingkungan
- Perlindungan produk dari cuaca dan kondisi buruk lainnya
- Pastikan proses internal didefinisikan dan dikendalikan

Penggunaan standar kualitas bersifat opsional, tetapi pemangku kepentingan tertentu dapat diharapkan untuk melakukannya. Selain itu, beberapa organisasi atau lembaga pemerintah mungkin meminta pemasok dan mitranya untuk menggunakan standar tertentu sebagai syarat dalam menjalankan bisnis (Maria Khalid, 2013).

Estimasi fitur aplikasi yang mempengaruhi kualitas perangkat lunak didukung oleh model kualitas perangkat lunak. Komponen mendasar dari proses manajemen yang memastikan bahwa sistem memiliki sedikit kekurangan dan memenuhi harapan adalah kualitas produk. Kualitas dari lima sudut yang berbeda, diantaranya (Maria Khalid, 2013):

1. Gagasan transendental bahwa Keunggulan adalah sesuatu yang dapat dihargai tetapi tidak dapat dijelaskan
2. Interpretasi pengguna: Kualitas adalah kesesuaian untuk tujuan,
3. Kualitas dalam manufaktur adalah kepatuhan terhadap spesifikasi,
4. Tampilan produk, yang menyiratkan bahwa Kualitas terkait dengan kualitas dasar suatu produk
5. Perspektif berbasis nilai menyiratkan hal itu

12.3 Mengapa Standar Penting?

Untuk bisnis: Intinya setiap organisasi bergantung pada standar. Bisnis yang sukses memahami perlunya mengelola standar bersama dengan kualitas, keamanan, kekayaan intelektual, dan peraturan lingkungan. Dengan membatasi kesalahan atau penarikan kembali, mengurangi redundansi, dan mempercepat waktu pemasaran, standardisasi menurunkan biaya (Asq.org, 2022).

Untuk kepentingan ekonomi global, perusahaan dan organisasi yang mematuhi standar kualitas memungkinkan pergerakan barang, jasa, dan manusia lintas batas. Mereka juga menjamin bahwa barang-barang yang dibuat di satu negara dapat dibeli dan digunakan di negara lain. Untuk pengguna barang dan jasa: Banyak standar manajemen mutu menawarkan perlindungan, tetapi standardisasi juga dapat membuat hidup pelanggan lebih mudah. Item atau layanan yang dibangun dengan standar internasional akan berfungsi dengan lebih banyak item atau layanan secara global, memperluas jangkauan opsi yang tersedia di mana saja. (Asq.org, 2022)

Di perusahaan mana pun, jaminan kualitas adalah yang paling penting. Koreksi kesalahan setelah pengiriman produk sangat mahal dan menantang. Standar Jaminan Kualitas harus dipertahankan untuk memastikan kualitas produk untuk menghindari masalah ini. Beberapa Standar Kualitas diikuti oleh organisasi TI, dan beberapa perusahaan ini juga menggunakan alat evaluasi Kualitas untuk Jaminan Kualitas. Berikut ulasan tentang Standar Kualitas di Industri IT (Maria Khalid, 2013).

12.3.1 Evaluasi kualitas untuk metodologi Model-Driven Web Engineering

Beberapa pendekatan telah digunakan dalam MDWE untuk merancang aplikasi web (*Model-Driven Web Engineering*). Mengingat metodologi ini berisi prosedur dan metode untuk membuat aplikasi web, sangat penting untuk mendeteksi dan meningkatkan kualitas dalam pendekatan ini. Berdasarkan standar ISO/IEC (*International Organization for Standardization/International Electro technical Commission*), penelitian ini bermaksud untuk mendefinisikan karakteristik Kualitas dan sub karakteristik untuk teknik MDWE. Efisiensi dan kualitas teknik MDWE ditingkatkan oleh karakteristik dan sub karakteristik Kualitas ini, yang juga menilai kesalahan dan kekuatan pendekatan (Maria Khalid, 2013).

12.3.2 Evaluasi Faktor Jaminan Kualitas dalam Metodologi Agile

Pengembangan perangkat lunak tangkas menegaskan bahwa itu akan meningkatkan kaliber keluaran perangkat lunak. Penegasan ini telah mengarah pada penerapannya dalam bisnis perangkat lunak yang muncul dan dalam teknologi informasi, tetapi hanya sedikit kerangka kerja untuk mengevaluasi kualitas yang tersedia karena masih mudanya industri ini. Alat baru untuk mengevaluasi kualitas dalam pengembangan perangkat lunak tangkas dikembangkan melalui penelitian, namun kelayakannya untuk penggunaan komersial belum ditetapkan. Alat yang disarankan menawarkan berbagai metode yang dapat digunakan untuk menilai berbagai aspek kualitas perangkat lunak. Alat yang diusulkan menciptakan platform baru untuk berbagai pengujian dalam metodologi tangkas dan juga membuka perspektif baru studi di industri perangkat lunak (Maria Khalid, 2013).

12.3.3 Bagaimana meningkatkan penjaminan mutu perangkat lunak di negara-negara miskin

Industri perangkat lunak sangat mementingkan kualitas. Kebahagiaan pelanggan, yang dapat dicapai dengan menerapkan standar, menentukan kualitas perangkat lunak. Studi ini menunjukkan dengan tepat masalah yang mencegah otoritas yang lebih tinggi untuk meningkatkan kualitas perangkat lunak. Permasalahan yang ditemukan dalam penelitian ini antara lain kurangnya profesional, pola pikir developer, tenggat waktu yang tidak masuk akal, standarisasi yang kurang, pembentukan tim dan kompromi kualitas, dan politik internal. Penelitian menyarankan metode berikut untuk mengatasi masalah ini: penerapan model CMMI; tim SQA yang berkualitas dan terspesialisasi; mencengkeram pengetahuan domain; tidak ada kompromi pada kualitas; dan pola pikir pengembang yang tepat (Maria Khalid, 2013).

12.3.4 Standar & Spesifikasi Kualitas Konstruksi Soft-Scape di Malaysia

Standar dan spesifikasi untuk konstruksi soft-scape tercakup. Organisasi pemerintah dan perusahaan komersial tertentu telah memberikan dokumen yang sebanding untuk perbandingan. Yang dibahas adalah perbedaan antara kualitas produk dan proses. Sementara "Kualitas Produk" berurusan dengan produk yang diproduksi sesuai dengan desain dan spesifikasi, "Kualitas Proses" berkaitan dengan ketergantungan teknik dan keterampilan pengembang. Laporan studi ini pada dasarnya meneliti bagaimana standar yang sebanding diterapkan secara berbeda oleh berbagai bisnis, yang mengarah ke hasil yang bervariasi untuk berbagai perusahaan (Maria Khalid, 2013).

12.3.5 Menganalisis keefektifan dan ketergantungan sistem jaminan kualitas courseware E-learning

E-learning, sering dikenal sebagai pembelajaran elektronik, semakin populer setiap hari. Karena jarak yang sangat jauh, penjaminan mutu dalam kursus e-learning menjadi lebih penting. Sertifikasi Kualitas E-learning dinilai, dan validitas prosedur sertifikasi diperiksa di Taiwan menggunakan metodologi yang digunakan oleh eLQSC (Pusat Layanan Kualitas *e-Learning*). Enam puluh tujuh aplikasi courseware E-learning dievaluasi menggunakan alat evaluasi eLCQC (*e-Learning Courseware Quality Checklist*). Teknik evaluasi eLCQC menunjukkan keandalan yang cukup, kompleksitas item, dan diskriminasi item. Alamat email yang Anda masukkan sudah pernah digunakan (Maria Khalid, 2013).

12.3.6 Jaminan Kualitas untuk Perangkat Lunak studi berdasarkan industri perangkat lunak di Pakistan

Praktik manajemen kualitas sangat penting dalam industri perangkat lunak. Tinjauan literatur mengidentifikasi aspek-aspek penting dari manajemen mutu di sektor perangkat lunak, yang kemudian didukung oleh penyelidikan eksperimental. Atas dasar aspek krusial manajemen kualitatif, dibuat perbandingan antara perusahaan yang lebih berpengalaman dan kurang berpengalaman. Studi ini menunjukkan bagaimana dampak "usia Kualitas" dan "penggunaan perangkat lunak" pada strategi manajemen Kualitas perangkat lunak diselidiki. Hasil penelitian menunjukkan bahwa "usia perangkat lunak" dan "penggunaan perangkat lunak" memiliki pengaruh yang kecil terhadap manajemen kualitas perangkat lunak. Untuk bersaing dengan sektor perangkat lunak lain dalam hal kualitas produk, bisnis perangkat lunak Pakistan harus meningkatkan metode manajemen kualitas perangkat lunak mereka (Maria Khalid, 2013).

12.3.7 Metode Kuadrat Terkecil Logaritmik Fuzzy: Metodologi Proses Hierarki Analitik Grup Fuzzy untuk Manajemen Penjaminan Kualitas Perangkat Lunak

Metode *Fuzzy Group Analytical Hierarchy Process* digunakan untuk mengevaluasi kualitas perangkat lunak. *International Organization for Standardization* (ISO/IEC9126-1:2001), yang terdiri dari enam kriteria dan dua puluh tujuh sub kriteria, digunakan sebagai standar internasional untuk atribut kualitas perangkat lunak. Relevansi vektor bobot diperoleh dengan menggunakan metode *fuzzy Logarithmic Least Squares* (LLSM) yang dimodifikasi, yang merupakan teknik prioritas. Untuk membuat kriteria rating dalam bilangan *fuzzy*, *Fuzzy Prioritization Programming for Direct Rating Scales* (FPP-DRS) dan fungsi penskalaan diusulkan. Metode ini akan membantu pemrogram, penguji, dan pembeli dalam menilai kualitas perangkat lunak dan meningkatkan efisiensi proses (Maria Khalid, 2013).

12.3.8 Implementasi dan Konfigurasi Model Manajemen Peningkatan Mutu Perguruan Tinggi

Kualitas Pakistan dan negara berkembang lainnya memiliki kebutuhan dasar untuk pendidikan dan perbaikan sistem pendidikan mereka. Memperkenalkan gagasan kontribusi rasional dari generasi muda memperkuat sistem pendidikan. Untuk menciptakan inisiatif yang unik, siswa muda membutuhkan bimbingan karena mereka tidak memiliki pengetahuan tentang pekerjaan sebelumnya di lapangan. Perguruan Tinggi tidak diberikan wadah untuk menyimpan informasi tentang karya mahasiswa. Studi ini menyajikan model konfigurasi untuk masalah tersebut, yang mengusulkan bahwa ketika permintaan untuk pendidikan tinggi terkait proyek dibuat, unit kontrol harus memeriksa penyimpanan

data dan menginformasikan kepada pemohon tentang status proyek serta pekerjaan terkait yang telah dilakukan. dokumentasi yang telah selesai dan dikelola. dengan mempraktikkan model konfigurasi Kualitas proyek meningkat, dan mendorong siswa untuk menghasilkan karya kreatif (Maria Khalid, 2013).

12.3.9 Menggunakan Model Kualitas ISO 9126 untuk menilai aplikasi bisnis-ke-bisnis

Aplikasi web dievaluasi dengan menggunakan model kualitas perangkat lunak. Aplikasi web dievaluasi menggunakan metodologi ISO 9126, yang disesuaikan untuk aplikasi B2B (*Business-to-Business*). Faktor kualitas diekstraksi setelah analisis aplikasi web. Dengan menghapus dan menilai aspek Kualitas dari aplikasi online dan aplikasi B2B, kustomisasi tercapai. Elemen Kualitas ini disertakan dalam model ISO 9126 dan diperhitungkan baik dari perspektif pengembang maupun akhir. pengguna (Maria Khalid, 2013)

12.3.10 Framework dan aplikasi untuk mengintegrasikan RFID dengan sistem Quality Assurance

Sistem jaminan kualitas sangat penting untuk menangani anomali, memeriksa kualitas produk, dan mengembangkan strategi peningkatan. Teknologi RFID membantu sistem Jaminan Kualitas dalam mengidentifikasi dan mencegah masalah kualitas. RFID sebagai sistem Jaminan Kualitas jauh lebih efektif daripada QAS tradisional lainnya dalam meningkatkan kualitas produk. Kerangka kerja dibuat untuk QAS (Sistem Jaminan Kualitas) berbasis RFID, yang membantu karyawan di lokasi dalam menangani penyimpangan dan kesalahan serta mengendalikan perubahan selama proses produksi. RFID terbukti sangat membantu dalam

memenuhi standar layanan pelanggan dan kontrol kualitas (Maria Khalid, 2013).

12.4 Mengapa Standar Dari ASQ?

Pengembangan standar internasional sangat dibantu oleh ASQ. Tanggung jawab ASQ adalah mengawasi *Technical Advisory Groups* (TAGs) di Amerika Serikat yang menciptakan standar paling terkenal, termasuk ISO 9001, ISO 19011, ISO 26000, dan ISO 14001. Bagi orang dan organisasi yang ingin meningkatkan penggunaan dan sesuai dengan standar kualitas, ASQ juga membuat buku, artikel, studi kasus, webcast, pelatihan, dan materi tambahan lainnya.

12.5 Kesimpulan

Standar jaminan kualitas sangat penting untuk menangani ketidaknormalan, menilai kualitas produk, dan mengembangkan strategi perbaikan. Standar ini sangat penting untuk memastikan kepuasan pelanggan dan sertifikasi kualitas industri TI. Dalam penelitian ini, dipelajari beberapa Standar Penjaminan Mutu yang diikuti oleh berbagai industri TI. Beberapa industri menganut standar kualitas ini untuk menjamin kualitas dalam proses produksi mereka dan untuk menghasilkan barang berkualitas tinggi yang memenuhi semua persyaratan standar. Seri ISO 9000 Organisasi Internasional untuk Standardisasi digunakan oleh sebagian besar cara untuk mengatasi tantangan kualitas. CMMI (*Capability Maturity Model Integration)*, PMI (*Project Management Institute*), ANSI (*American National Standards Institute*), ISO/IEC (*International Electro technical Commission*), DRR (*Digitally Reconstructed Radiography),* dan ASQ adalah metodologi lebih lanjut (*American Society of Quality*). Semua sektor TI yang lebih mementingkan mendapatkan kualitas mematuhi standar sesuai dengan kebutuhan sistemnya. Beberapa teknik juga

menggunakan alat evaluasi Kualitas untuk Jaminan Kualitas seperti alat QAS berbasis RFID (*Radio-frequency Identification*) yang membantu staf di lapangan untuk mengontrol perubahan selama proses produksi dan menangani ketidaknormalan dan cacat, alat eLCQC (*e-Learning Courseware Quality Checklist*) digunakan untuk evaluasi kualitas aplikasi E-learning courseware. Penerapan berbagai standar kualitas oleh berbagai industri TI diperiksa dalam penelitian ini, dan setelah standar ini dimasukkan ke dalam sistem perusahaan tersebut, sistem tersebut telah meningkat. Karena kendala keuangan mereka, beberapa industri TI merasa sulit untuk mematuhi Standar Kualitas untuk Menjamin Kualitas. Bisnis dan industri di bidang TI menggunakan standar sesuai dengan domain yang relevan untuk memenuhi kriteria kualitasnya. Beberapa perusahaan multinasional juga membuat standarnya sendiri, awalnya berfokus pada layanan. Saat ini, mencapai kualitas sangat penting karena meningkatnya harapan klien. Karena sebagian besar perusahaan tidak memandang kualitas sebagai faktor penting, yang menyebabkan penurunan awal mereka dan merupakan salah satu kelemahan utama mereka, disarankan agar industri TI mengikuti kegiatan jaminan kualitas untuk memenuhi standar kualitas guna meningkatkan kualitas produk mereka. Industri dengan sertifikasi standar memberikan nilai tambah bagi pasar domestik dan global serta memenuhi permintaan klien (Maria Khalid, 2013).

DAFTAR PUSTAKA

Asq.org. 2022. *SUMBER KUALITAS,asq.org*. Tersedia di: https://asq.org/ (Diakses: 15 Maret 2023).

Manghani, K. 2011. 'Jaminan kualitas: Pentingnya sistem dan prosedur operasi standar',*Perspektif dalam Penelitian Klinis*, 2(1), hal.34. doi: 10.4103/2229-3485.76288.

Maria Khalid, M.K. 2013. 'Standar Penjaminan Mutu dan Survei Industri TI',*Jurnal Teknik Komputer IOSR*, 10(2), hlm. 65–74. dua: 10,9790/0661-01026574.

BIODATA PENULIS

Wahyuddin S, S.Kom., M.Kom
Dosen STMIK Amika Soppeng

Wahyuddin S. was born at Malaka-Bone-Sulawesi Selatan in 1992. In 2011 he attended STMIK Dipanegara Makassar and was completed in 2015. He was completed after attending 7 semesters and active on an XPcom (Extreme Programmer Computer) campus organization. He was also active as a lecturer assistant for three semesters and taught several courses on programming. He continued his Master of Information systems at UNIKOM Bandung in 2016 and was completed in April 2019. He worked as a lecturer at a campus (STMIK Amika Soppeng) 2019 to present and also a Freelance Web Programmer. Has competence in the field of software engineer, application developer, multimedia, web developer, network security, and data analyst.

BIODATA PENULIS

Nono Heryana, M. Kom.
Dosen Program Studi Sistem Informasi
Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang

Penulis lahir di Lampung Barat tanggal 03 Maret 1989. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika di Universitas Singaperbangsa Karawang lulus tahun 2012 dan melanjutkan S2 pada Jurusan Ilmu Komputer di Universitas Budi Luhur lulus tahun 2016. Selain menempuh pendidikan formal penulis juga memiliki beberapa sertifikasi profesi, baik lokal maupun internasional. Seperti: *Google Certified Educator Level 1*, *Certified International of Internal Quality Audit (CIIQA)*, *Scrum Master Accredited Certification™ (SMAC), Scrum Foundation Professional Certificate (SFPC), Certified of Editor (C. Ed), Certified Business Operations Associate (CBOA®)* dan *Remote Worker Professional Certificate (RWPC)*. Penulis adalah dosen tetap pada Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Singaperbangsa Karawang, sejak tahun 2016 sampai dengan sekarang.

BIODATA PENULIS

Alexander Waworuntu, S.Kom., M.T.I.
Dosen Informatika, Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis lahir di Surabaya pada tanggal 9 Juni. Penulis adalah dosen pada Program Studi Informatika, Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada jurusan Teknik Informatika pada tahun 2006 di Universitas Bina Nusantara. Selanjutnya penulis menyelesaikan pendidikan S2 pada program studi Magister Teknologi Informasi di Universitas Indonesia pada tahun 2012.

BIODATA PENULIS

Abdurrasyid, S.Kom., MMSI.
Dosen Program Studi Teknik Informatika
Fakultas Telematika Energi Institut Teknologi PLN

Penulis lahir di Jakarta tanggal 10 Juni 1987. Saat ini penulis menjadi dosen tetap pada Program Studi Teknik Informatika, Fakultas Telematika Energi, Institut Teknologi PLN Jakarta. Penulis aktif melakukan publikasi dalam berbagai jurnal ilmiah baik nasional maupun internasional, memiliki ketertarikan pada bidang software engineering dan machine learning, dan saat ini penulis sedang melanjutkan studinya di Institut Teknologi Bandung.

BIODATA PENULIS

Angga Aditya Permana
Dosen Program Studi Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS

Rima Rizqi Wijayanti, S.ST., MMSI.
Dosen Program Studi Teknik Informatika
Fakultas Teknik, Universitas Muhammadiyah Tangerang

Penulis lahir di Jakarta tanggal 22 Mei 1986. Saat ini penulis merupakan dosen tetap pada Program Studi Teknik Informatika Fakultas Teknik, Universitas Muhammadiyah Tangerang. Penulis menyelesaikan pendidikan S1 di STMI Jakarta dan melanjutkan S2 di Universitas Gunadarma pada Tahun 2017, serta memiliki ketertarikan pada bidang sistem informasi.

BIODATA PENULIS

Dr. Santo Fernandi Wijaya., S.Kom., M.M.
Dosen Program Studi Sistem Informasi,
Fakultas Teknik dan Informatika,
Universitas Multimedia Nusantara, Tangerang.

Penulis lahir di Jakarta dan sebagai dosen tetap pada Program Studi Sistem Informasi Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara, Tangerang. Penulis menyelesaikan pendidikan studi Strata-1 Jurusan Komputerisasi Akuntansi, Universitas Bina Nusantara, Jakarta (1994). Strata-2 Jurusan Sistem Informasi, Universitas Bina Nusantara, Jakarta (2000). Strata-3 Jurusan Doctor Computer Science, Universitas Bina Nusantara, Jakarta (2022). Penulis telah menulis beberapa buku mengenai ERP dan solusi bisnis. Disamping itu, penulis telah memiliki pengalaman pada tingkatan manajerial sebagai praktisi selama 34 tahun (1988 sd 2022) dalam bidang Finance, Accounting, dan berpengalaman mengimplementasikan sistem ERP pada beberapa perusahaan industri manufaktur. Penulis aktif sebagai dosen praktisi pada prodi Sistem Informasi di Binus University sejak tahun 2001. Penulis aktif melakukan riset dalam bidang Enterprise System, Knowledge Management, Business Process Management,

Change Management, Analisis dan pengembangan sistem informasi. Penulis dapat dihubungi dengan email: santofwijaya@gmail.com, Google scholar ID: wbwFg.AAAAAJ, https://orcid.org/0000-0002-0650-2066, Sinta ID: 6009307, Scopus ID: 57194540113.

BIODATA PENULIS

Suwito Pomalingo, S.Kom., M.Kom.
Dosen Program Studi Informatika
Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Magister Informatika Universitas Islam Indonesia.

Saat ini sementara menyelesaikan studi Doktoral dengan topik penelitian di bidang Security Science dengan pendekatan Deep Learning. Penulis menekuni bidang keilmuan meliputi Cyber Security, Malware Analytics, Data Science, Machine Learning, dan Deep Learning, selain itu, penulis juga memiliki beberapa serifikasi internasional di bidang Cyber Security, Digital Forensics, Data Science dan Machine Learning.

BIODATA PENULIS

Alfrian C Talakua, S.SI., M.Kom
Dosen Program Studi Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Kristen Wira Wacana Sumba

Penulis Penulis lahir di Ambon tanggal 14 Oktober 1993. Penulis adalah dosen tetap pada Program Studi Teknik Informatika Fakultas Sains dan Teknologi, Universitas Kristen Wira Wacana Sumba. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi dan melanjutkan S2 pada Jurusan yang sama Sistem Informasi pada Universitas Kristen Satya Wacana Salatiga. Penulis menekuni Bidang Rekayasa Perangkat Lunak, Web Developer, Tata Kelola IT dan pengembangan skill terkait bidang Sistem Informasi Geografis dalam menunjang penelitan di Sumba.

BIODATA PENULIS

Agung Susilo Yuda Irawan, M.Kom.
Dosen Program Studi Informatika
Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang

Penulis lahir di Kuningan tanggal 15 Juni 1993. Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Ilmu Komputer Universitas Singaperbangsa Karawang. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Magister Ilmu Komputer.

BIODATA PENULIS

Dr. Luluk Tri Harinie, SE., MM
Dosen Jurusan Manajemen
Fakultas Ekonomi dan Bisnis
Universitas Palangka Raya

Penulis lahir di Palangka Raya tanggal 22 Juli 1972. Penulis adalah dosen tetap pada Jurusan Manajemen Fakultas Ekonomi dan Bisnis, Universitas Palangka Raya. Menyelesaikan pendidikan Sarjana Ekonomi (SE) di STIE Malangkuçeçwara Malang (1995) pada program studi Manajemen. Selanjutnya menempuh pendidikan Magister (2004) dan pendidikan Program Doktor (2018) di Universitas Brawijaya Malang pada program Studi Ilmu Manajemen. Dan saat ini berkarier menjadi Staf Pengajar (Dosen) pada Jurusan Manajemen Fakultas Ekonomi dan Bisnis Universitas Palangka Raya. Penulis menekuni bidang ilmu Manajemen Pemasaran dan Kewirausahaan.

BIODATA PENULIS

Wirawan Istiono, S.Kom., M.Kom.
Dosen Informatika
Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara

Penulis lahir di Jakarta tanggal 13 April 1983. Penulis adalah dosen pada Program Studi Informatika Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada bidang jurusan yang Teknik Informatika. Pada saat ini, penulis menekuni bidang Penelitian terkait komputer sains, sistem komputer dan teknologi informasi