Proses Pencapaian dan Pemeliharaan Kepatuhan terhadap Regulasi TI

DISUSUN OLEH:

BAGUS SADEWA	**2217020005**
KHAIRIL RAHMAN HAKIKI HRP.	**2217020020**

DOSEN PENGAMPU :

HADITYA PRASETYO, S.Kom, M.Kom

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS SAINS DAN TEKNOLOGI

UIN IMAM BONJOL PADANG

2025

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan makalah dengan judul "Proses Pencapaian dan Pemeliharaan Kepatuhan terhadap Regulasi TI Berdasarkan Perspektif Wheeler (2011)" dengan baik dan tepat waktu. Makalah ini disusun sebagai salah satu bentuk pemahaman dan pendalaman materi perkuliahan terkait manajemen risiko TI, khususnya pada aspek kepatuhan, etika, dan ketahanan sistem.

Dalam penyusunan makalah ini, penulis menggunakan referensi utama dari Evan Wheeler melalui karyanya yang berjudul *Security Risk Management* (2011). Buku tersebut memberikan landasan teoretis yang komprehensif mengenai penerapan prinsip-prinsip etika dalam manajemen risiko, termasuk perlindungan privasi pengguna dan data pribadi. Selain itu, makalah ini juga mengulas bagaimana mengevaluasi dampak keputusan manajemen risiko terhadap berbagai pemangku kepentingan (*stakeholders*), serta menjelaskan konsep *Disaster Recovery Center* (DRC) sebagai strategi vital dalam menjamin ketersediaan layanan. Pemahaman terhadap konsep-konsep tersebut menjadi sangat penting mengingat tantangan regulasi TI saat ini menuntut pendekatan yang lebih dari sekadar pemenuhan daftar periksa.

Penulis menyampaikan terima kasih kepada dosen pengampu mata kuliah serta seluruh pihak yang telah memberikan bimbingan, dukungan, dan motivasi sehingga makalah ini dapat terselesaikan. Penulis menyadari bahwa makalah ini masih memiliki keterbatasan, baik dari segi penulisan maupun kedalaman analisis. Oleh karena itu, kritik dan saran yang bersifat membangun sangat penulis harapkan demi penyempurnaan karya ilmiah di masa yang akan datang.

Padang, 2 Desember 2025

Penulis

DAFTAR ISI

KATA PENGANTAR 2
DAFTAR ISI 3
BAB I PENDAHULUAN 5
1.1 Latar Belakang 5
1.2 Rumusan Masalah 6
1.3 Tujuan Penulisan 7
1.4 Manfaat Penulisan 7
BAB II PEMBAHASAN 8
2.1 Proses Pencapaian dan Pemeliharaan Kepatuhan Melalui *Security Risk Reviews* 8
2.1.1 Metodologi *Gap Analysis* dalam Kepatuhan 8
2.1.2 Siklus Hidup Kepatuhan (*Compliance Lifecycle*) 9
2.1.3 Pendekatan NIST untuk Pemeliharaan Berkelanjutan 10
2.2 Penerapan Etika dan Perlindungan Privasi dalam Manajemen Risiko 10
2.2.1 Prinsip Etika Dasar: *Safety before Security* 10
2.2.2 Profiling Risiko untuk Data Sensitif dan Privasi 11
2.2.3 Penyeimbangan Kontrol Keamanan dan Hak Privasi 11
2.3 Evaluasi Dampak Keputusan Risiko Terhadap Pemangku Kepentingan (*Stakeholders*) 12
2.3.1 Pemetaan Risiko ke Tujuan Bisnis 12
2.3.2 Peran Keamanan dalam Pengambilan Keputusan (*Facilitating Decision Making*) 13
2.3.3 Manajemen Pengecualian (*Exception Management*) 13
2.4 Konsep Ketahanan (Resilience) dan Disaster Recovery Center 16
2.4.1 Konsep Dasar *Resilience* 16
2.4.2 Strategi dan Arsitektur *Disaster Recovery* 17
2.4.3 Evaluasi Kelangsungan Bisnis Pihak Ketiga 17

BAB III KESIMPULAN 19
3.1 Kesimpulan 19
3.2 Saran 20

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam lanskap teknologi informasi (TI) yang terus berkembang, paradigma keamanan informasi telah bergeser dari pendekatan yang murni berorientasi teknis menjadi pendekatan berbasis manajemen risiko bisnis. Wheeler (2011) dalam bukunya *Security Risk Management* menegaskan bahwa keamanan informasi tidak lagi sekadar tentang *firewall*, enkripsi, atau kepatuhan buta terhadap daftar periksa (*checklist*). Sebaliknya, tujuan utama keamanan informasi adalah memastikan kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan akuntabilitas (*accountability*) atau disingkat C-I-A-A sumber daya organisasi tetap berada pada tingkat risiko yang dapat diterima.

Tantangan terbesar yang dihadapi organisasi saat ini adalah mencapai dan memelihara kepatuhan terhadap regulasi TI yang semakin ketat tanpa menghambat operasional bisnis. Banyak organisasi terjebak dalam mentalitas "kepatuhan demi kepatuhan", di mana mereka merasa aman hanya karena telah memenuhi standar regulasi, padahal kepatuhan tidak selalu menjamin keamanan (Wheeler, 2011). Proses pencapaian kepatuhan sering kali dilakukan secara ad-hoc atau reaktif, padahal yang dibutuhkan adalah proses yang berkelanjutan dan sistematis, seperti *Security Risk Reviews* (SRR), untuk mengidentifikasi kesenjangan (*gap analysis*) antara standar yang ditetapkan dengan praktik di lapangan.

Di sisi lain, manajemen risiko TI tidak dapat dipisahkan dari prinsip-prinsip etika. Keputusan untuk melindungi atau tidak melindungi aset informasi memiliki dampak langsung pada privasi pengguna dan perlindungan data pribadi. Wheeler (2011) menekankan prinsip *"Safety before Security"*, di mana kontrol keamanan tidak boleh membahayakan keselamatan manusia atau melanggar hak privasi individu. Dalam konteks regulasi seperti HIPAA atau standar industri seperti PCI-DSS, kegagalan dalam melindungi data sensitif bukan hanya masalah teknis, melainkan pelanggaran etika yang dapat merusak kepercayaan publik dan reputasi organisasi.

Selain itu, setiap keputusan manajemen risiko mulai dari penerimaan risiko (*risk acceptance*) hingga mitigasi memiliki dampak signifikan terhadap berbagai pemangku kepentingan (*stakeholders*), termasuk eksekutif, pemilik aset, hingga pengguna akhir. Manajer risiko harus mampu memfasilitasi pengambilan keputusan yang menyeimbangkan biaya kontrol dengan nilai aset yang dilindungi. Keputusan yang diambil tanpa mempertimbangkan dampak bisnis dapat menyebabkan pemborosan sumber daya atau, sebaliknya, eksposur risiko yang tidak terkendali.

Terakhir, dalam kerangka C-I-A-A, aspek ketersediaan (*availability*) menuntut organisasi untuk memiliki ketahanan (*resilience*) terhadap gangguan operasional. Di sinilah konsep *Disaster Recovery Center* (DRC) menjadi krusial. DRC bukan sekadar fasilitas cadangan, melainkan wujud dari strategi manajemen risiko untuk menjamin kelangsungan bisnis saat terjadi bencana. Kepatuhan terhadap regulasi TI sering kali mewajibkan adanya redundansi dan rencana pemulihan yang teruji untuk meminimalkan dampak gangguan terhadap layanan kritis.

Berdasarkan uraian di atas, makalah ini akan membahas secara mendalam proses pencapaian dan pemeliharaan kepatuhan regulasi TI dengan pendekatan manajemen risiko menurut Evan Wheeler, dengan penekanan khusus pada etika privasi, dampak terhadap pemangku kepentingan, serta ketahanan sistem melalui konsep *Disaster Recovery Center*.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam makalah ini adalah sebagai berikut:

1. Bagaimana proses pencapaian dan pemeliharaan kepatuhan terhadap regulasi TI dilakukan melalui pendekatan *Security Risk Reviews* dan *Gap Analysis*?
2. Bagaimana prinsip-prinsip etika diterapkan dalam manajemen risiko TI untuk menjamin perlindungan data pribadi dan privasi pengguna?
3. Bagaimana cara mengevaluasi dampak keputusan manajemen risiko TI terhadap berbagai pemangku kepentingan (*stakeholders*) dalam organisasi?

4. Bagaimana konsep *Disaster Recovery Center* (DRC) dijelaskan sebagai bagian dari strategi ketahanan (*resilience*) dan ketersediaan (*availability*) dalam arsitektur keamanan?

1.3 Tujuan Penulisan

Tujuan dari penyusunan makalah ini adalah:

1. Menjelaskan metodologi pencapaian dan pemeliharaan kepatuhan regulasi TI menggunakan siklus hidup tinjauan risiko (*Security Risk Reviews*) dan pendekatan NIST sesuai pandangan Wheeler.
2. Menganalisis penerapan etika dalam manajemen risiko, khususnya terkait prinsip *safety before security* dan perlindungan terhadap informasi sensitif (privasi).
3. Mengevaluasi dampak dari keputusan risiko (mitigasi, transfer, atau penerimaan risiko) terhadap kepentingan bisnis dan *stakeholder*.
4. Mendeskripsikan konsep, strategi, dan arsitektur *Disaster Recovery Center* (DRC) sebagai kontrol fundamental untuk menjamin ketersediaan layanan.

1.4 Manfaat Penulisan

Penulisan makalah ini diharapkan dapat memberikan manfaat sebagai berikut:

1. **Manfaat Teoritis:**

   Menambah wawasan akademik mengenai integrasi antara manajemen kepatuhan (*compliance*), etika profesi keamanan, dan arsitektur ketahanan sistem berdasarkan literatur *Security Risk Management* (2011).

2. **Manfaat Praktis:**

   Memberikan panduan bagi praktisi TI dan mahasiswa dalam merancang program manajemen risiko yang tidak hanya patuh terhadap regulasi, tetapi juga etis dalam menangani data privasi serta tangguh dalam menghadapi bencana melalui implementasi DRC yang tepat.

BAB II
PEMBAHASAN

2.1 Proses Pencapaian dan Pemeliharaan Kepatuhan Melalui *Security Risk Reviews*

Dalam manajemen risiko keamanan informasi, kepatuhan (*compliance*) terhadap regulasi bukanlah tujuan akhir, melainkan konsekuensi dari praktik keamanan yang baik. Wheeler (2011) menekankan bahwa menerbitkan kebijakan keamanan saja tidak cukup; organisasi harus secara aktif menilai apakah standar tersebut diterapkan secara efektif. Metode utama yang diusulkan untuk mencapai dan memelihara kepatuhan ini adalah melalui **Security Risk Reviews (SRR)**.

2.1.1 Metodologi *Gap Analysis* dalam Kepatuhan

Security Risk Review (SRR) pada dasarnya adalah sebuah latihan analisis kesenjangan (*gap analysis*). Berbeda dengan audit yang sering kali bersifat menghakimi dan kaku, SRR dirancang sebagai proses kolaboratif antara tim keamanan informasi dan pemilik bisnis (*business owners*).

Proses ini membandingkan dua kondisi utama:

1. **Standar Aktif (*Active Standards*):** Apa yang tertulis dalam kebijakan dan regulasi yang berlaku (seperti ISO 27001, PCI-DSS, atau kebijakan internal).
2. **Praktik Saat Ini (*Current Practices*):** Apa yang sebenarnya terjadi di lapangan dalam operasional sehari-hari.

Wheeler (2011: 239) menjelaskan bahwa tujuan SRR bukan untuk mencari kesalahan, melainkan untuk mengidentifikasi area di mana terdapat penyimpangan (*deviation*) dan menentukan apakah penyimpangan tersebut dapat diterima oleh organisasi. Dalam konteks regulasi TI, tidak semua kontrol harus diterapkan dengan cara yang persis sama ("*cookbook approach*"). SRR memungkinkan organisasi untuk menyeimbangkan kebutuhan keamanan dengan risiko operasional, mencari kontrol kompensasi

(*compensating controls*) yang mungkin sudah ada dan memenuhi tujuan regulasi meskipun tidak sesuai dengan huruf standar secara teknis.

2.1.2 Siklus Hidup Kepatuhan (*Compliance Lifecycle*)

Untuk memelihara kepatuhan secara berkelanjutan, Wheeler (2011: 242) menguraikan alur kerja (*workflow*) yang sistematis. Proses ini memastikan bahwa kepatuhan bukan sekadar aktivitas tahunan, melainkan siklus yang hidup.

Tahapan dalam siklus ini meliputi:

1. **Penjadwalan dan Profiling:** Menentukan jadwal penilaian berdasarkan sensitivitas aset. Aset dengan risiko tinggi (misalnya yang memproses data regulasi) harus dinilai lebih sering.
2. **Kuesioner dan Wawancara:** Menggunakan instrumen standar untuk mengumpulkan data dari pemilik aset mengenai kepatuhan terhadap kontrol spesifik.
3. **Pembuatan Temuan (*Generate Findings*):** Mengidentifikasi item "Non-Compliant". Pada tahap ini, temuan diberi peringkat risiko awal (Low, Moderate, High, Critical).
4. **Kualifikasi Temuan:** Tim keamanan bekerja sama dengan pemilik aset untuk memvalidasi temuan. Seringkali, apa yang tampak sebagai pelanggaran regulasi sebenarnya telah dimitigasi oleh kontrol lain.
5. **Keputusan Risiko:** Ini adalah inti dari pemeliharaan kepatuhan. Organisasi memiliki tiga pilihan terhadap temuan ketidakpatuhan:
    - **Remidiasi:** Memperbaiki celah untuk mematuhi standar.
    - **Mitigasi:** Menerapkan kontrol alternatif untuk menurunkan risiko.
    - **Penerimaan (Exception):** Menerima risiko ketidakpatuhan secara formal dengan persetujuan manajemen senior.

2.1.3 Pendekatan NIST untuk Pemeliharaan Berkelanjutan

Selain SRR internal, Wheeler juga merujuk pada pendekatan **NIST (National Institute of Standards and Technology)**, khususnya SP 800-37, sebagai model ideal untuk memelihara kepatuhan regulasi yang kompleks. Pendekatan ini dikenal sebagai *Certification and Accreditation* (C&A).

Dalam model ini, pemeliharaan kepatuhan dilakukan melalui konsep **Continuous Monitoring**. Kepatuhan tidak dinilai hanya pada satu titik waktu (snapshot), tetapi dipantau secara terus-menerus. Setiap perubahan signifikan pada sistem (misalnya pembaruan perangkat lunak atau perubahan arsitektur jaringan) memicu evaluasi ulang terhadap status kepatuhan. Hal ini memastikan bahwa organisasi tidak "keluar dari kepatuhan" (*drift out of compliance*) seiring berjalannya waktu.

2.2 Penerapan Etika dan Perlindungan Privasi dalam Manajemen Risiko

Manajemen risiko TI tidak dapat dilepaskan dari pertimbangan etis. Keputusan teknis yang diambil oleh profesional keamanan memiliki dampak langsung terhadap hak individu, privasi, dan keselamatan manusia.

2.2.1 Prinsip Etika Dasar: *Safety before Security*

Prinsip etika paling fundamental yang ditekankan oleh Wheeler (2011: 8) adalah **"Safety before Security"**. Dalam upaya mematuhi regulasi atau mengamankan aset, organisasi tidak boleh menerapkan kontrol yang membahayakan keselamatan manusia.

Studi Kasus Etika Keselamatan:

Sebagai contoh, sebuah regulasi pusat data mungkin mengharuskan pintu akses terkunci secara otomatis (*fail-secure*) jika terjadi gangguan listrik untuk mencegah pencurian. Namun, secara etika dan keselamatan, jika terjadi kebakaran, pintu harus terbuka (*fail-safe*) agar personel dapat menyelamatkan diri. Profesional manajemen risiko harus memprioritaskan nyawa manusia di atas keamanan aset fisik atau data.

Kegagalan dalam menerapkan prinsip ini bukan hanya pelanggaran prosedur, tetapi pelanggaran etika profesi yang berat.

2.2.2 Profiling Risiko untuk Data Sensitif dan Privasi

Perlindungan data pribadi adalah kewajiban etis sekaligus legal. Wheeler (2011: 65) dalam pembahasan **Risk Profiling** (Chapter 4), menegaskan bahwa sensitivitas risiko tidak hanya diukur dari nilai aset bagi perusahaan, tetapi juga dampaknya terhadap pemilik data (pengguna/pelanggan).

Dalam melakukan *profiling*, organisasi harus secara spesifik mengidentifikasi keberadaan *Personally Identifiable Information* (PII) atau data sensitif lainnya. Wheeler menyarankan penggunaan kuesioner profil risiko (seperti pada **Appendix A**) yang secara eksplisit menanyakan:

- Apakah sistem menyimpan data kesehatan (terkait HIPAA)?
- Apakah sistem menyimpan data keuangan pribadi (terkait GLBA/PCI)?
- Jika data ini bocor, apa dampak reputasi dan legal bagi individu yang datanya terekspos?

Secara etis, organisasi harus mengasumsikan peran sebagai "penjaga" (*custodian*) data, bukan pemilik mutlak. Oleh karena itu, risiko kebocoran data harus dinilai berdasarkan kerugian yang akan diderita oleh subjek data, bukan hanya kerugian finansial perusahaan akibat denda regulasi.

2.2.3 Penyeimbangan Kontrol Keamanan dan Hak Privasi

Penerapan kontrol keamanan yang berlebihan (*over-control*) untuk mencapai kepatuhan dapat melanggar privasi pengguna. Wheeler memperingatkan agar tidak menciptakan "False Sense of Security" atau menerapkan pemantauan yang intrusif tanpa justifikasi yang kuat.

Misalnya, penerapan teknologi *monitoring* karyawan untuk mencegah kebocoran data (DLP) harus seimbang. Merekam setiap ketukan tombol (*keystroke*

logging) mungkin efektif untuk keamanan, namun secara etika hal tersebut melanggar privasi jika diterapkan secara menyeluruh tanpa batasan. Manajemen risiko yang etis harus mencari titik keseimbangan di mana tujuan keamanan tercapai tanpa mengorbankan hak privasi individu secara tidak proporsional.

2.3 Evaluasi Dampak Keputusan Risiko Terhadap Pemangku Kepentingan (*Stakeholders*)

Keputusan manajemen risiko baik itu memitigasi, mentransfer, atau menerima risiko tidak terjadi dalam ruang hampa. Setiap keputusan memiliki konsekuensi bagi berbagai pemangku kepentingan. Wheeler (2011: 148) menyoroti peran penting keamanan dalam memfasilitasi pengambilan keputusan bisnis.

2.3.1 Pemetaan Risiko ke Tujuan Bisnis

Untuk mengevaluasi dampak keputusan secara efektif, bahasa teknis risiko TI harus diterjemahkan ke dalam bahasa dampak bisnis yang dipahami oleh pemangku kepentingan.

Wheeler menyarankan evaluasi dampak berdasarkan kategori berikut:

1. **Finansial:** Dampak langsung berupa denda regulasi, biaya pemulihan, atau kehilangan pendapatan. Ini relevan bagi CFO dan pemegang saham.
2. **Reputasi:** Dampak terhadap kepercayaan merek (*brand trust*). Ini sangat relevan bagi tim Pemasaran dan Eksekutif (CEO), terutama dalam industri yang mengandalkan kepercayaan pelanggan seperti perbankan atau kesehatan.
3. **Legal & Regulasi:** Dampak hukum, termasuk tuntutan perdata atau pidana. Ini relevan bagi tim Legal dan *Compliance Officer*.
4. **Operasional:** Dampak terhadap kemampuan organisasi untuk memberikan layanan. Ini relevan bagi Manajer Operasional dan pengguna akhir.

2.3.2 Peran Keamanan dalam Pengambilan Keputusan (*Facilitating Decision Making*)

Wheeler (2011: 32) menegaskan bahwa tim keamanan tidak boleh menjadi pembuat keputusan tunggal atas risiko bisnis. Peran manajer risiko adalah sebagai **penasihat (advisor)** yang menyediakan data akurat kepada pemilik bisnis (*business owners*) agar mereka dapat membuat keputusan yang tepat (*informed decision*).

Jika sebuah regulasi mewajibkan enkripsi data namun biayanya sangat mahal dan akan memperlambat sistem, tim keamanan harus menyajikan analisis:

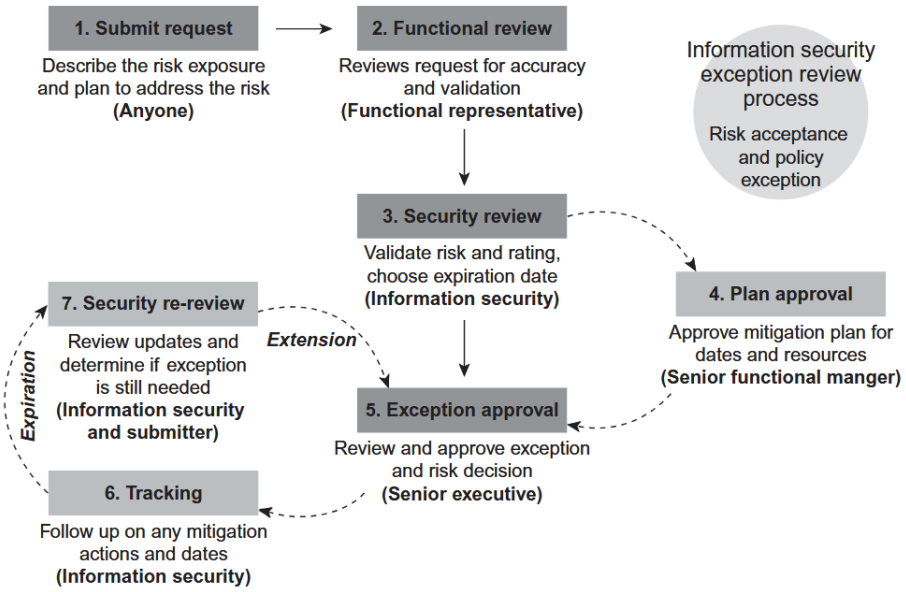
- Berapa biaya implementasi kontrol?
- Berapa potensi denda jika tidak patuh?
- Berapa besar kemungkinan pelanggaran terjadi?

Dengan data ini, pemangku kepentingan (misalnya Direktur Bisnis) dapat memutuskan apakah akan menginvestasikan dana untuk kontrol tersebut atau menerima risiko dengan catatan tertentu.

2.3.3 Manajemen Pengecualian (*Exception Management*)

Salah satu mekanisme terpenting untuk mengevaluasi dan mendokumentasikan dampak keputusan adalah melalui **Proses Pengecualian Kebijakan** (*Policy Exceptions*).

Wheeler (2011: 156) menjelaskan bahwa ketika bisnis memutuskan untuk *tidak* memitigasi risiko (misalnya karena alasan biaya atau fungsionalitas), keputusan tersebut harus didokumentasikan melalui pengecualian formal. Dokumen ini harus ditandatangani oleh pemangku kepentingan yang memiliki otoritas (misalnya C-Level Executive). Hal ini memastikan **akuntabilitas**; pemangku kepentingan sadar secara penuh akan konsekuensi (dampak) dari keputusan mereka menerima risiko tersebut, dan tidak bisa menyalahkan tim TI jika insiden terjadi di kemudian hari.



Gambar 2.3.3 *Risk exception approval workflow*

Sumber: Wheeler (2011: 158)

Gambar ini menunjukkan **Alur Kerja Persetujuan Pengecualian Risiko (Risk Exception Approval Workflow)**. Diagram ini menjelaskan langkah-langkah sistematis yang harus diambil oleh sebuah organisasi ketika ada kebutuhan untuk menyimpang dari kebijakan keamanan informasi standar atau ketika sebuah risiko keamanan harus diterima sementara waktu.

Berikut adalah penjelasan rinci untuk setiap langkah dalam diagram tersebut:

1. Pengajuan Permintaan (*Submit Request*)

- **Pelaku:** Siapa saja (*Anyone*) dalam organisasi.
- **Aktivitas:** Seseorang mengajukan permohonan pengecualian. Pengaju harus mendeskripsikan paparan risiko (*risk exposure*) yang ada dan rencana untuk menangani risiko tersebut.

2. Tinjauan Fungsional (*Functional Review*)

- **Pelaku:** Perwakilan Fungsional (*Functional Representative* - biasanya manajer lini atau atasan pengaju).

- **Aktivitas:** Memeriksa permintaan tersebut untuk memastikan akurasinya dan memvalidasi apakah kebutuhan bisnisnya masuk akal.

3. Tinjauan Keamanan (*Security Review*)

- **Pelaku:** Tim Keamanan Informasi (*Information Security*).
- **Aktivitas:** Tim keamanan memvalidasi risiko teknis dan memberikan peringkat risiko (*risk rating*). Di sini juga ditentukan tanggal kedaluwarsa (*expiration date*) untuk pengecualian tersebut, karena pengecualian seharusnya tidak berlaku selamanya.

4. Persetujuan Rencana (*Plan Approval*)

- **Pelaku:** Manajer Fungsional Senior (*Senior Functional Manager*).
- **Aktivitas:** Menyetujui rencana mitigasi (rencana perbaikan/pengurangan risiko), termasuk menyetujui tenggat waktu dan sumber daya (dana/tenaga) yang dibutuhkan untuk memperbaiki masalah tersebut.

5. Persetujuan Pengecualian (*Exception Approval*)

- **Pelaku:** Eksekutif Senior (*Senior Executive*).
- **Aktivitas:** Ini adalah tahap pengambilan keputusan final. Eksekutif meninjau permintaan dan secara resmi menyetujui pengecualian tersebut serta keputusan untuk menerima risiko (*risk acceptance*) atas nama perusahaan.

6. Pelacakan (*Tracking*)

- **Pelaku:** Tim Keamanan Informasi.
- **Aktivitas:** Memantau (mem-follow up) tindakan mitigasi yang telah disetujui dan memastikan tanggal-tanggal penyelesaian dipatuhi.

7. Tinjauan Ulang Keamanan (*Security Re-review*)

- **Pelaku:** Tim Keamanan Informasi dan Pengaju (*Submitter*).
- **Aktivitas:** Meninjau pembaruan status. Menentukan apakah pengecualian tersebut masih diperlukan atau masalah sudah teratasi.

- **Extension (Perpanjangan):** Jika pengecualian masih dibutuhkan setelah tanggal kedaluwarsa, proses akan kembali ke **Langkah 5** untuk meminta persetujuan ulang dari Eksekutif Senior.
- **Expiration (Kedaluwarsa):** Jika waktunya habis, status dipantau kembali (kembali ke langkah 6) atau ditutup jika risiko sudah dimitigasi.

Diagram ini bertujuan untuk menciptakan **Tata Kelola (Governance)** yang baik. Proses ini memastikan bahwa setiap penyimpangan dari aturan keamanan tidak dilakukan diam-diam, melainkan:

1. Didokumentasikan.
2. Dianalisis risikonya.
3. Disetujui oleh manajemen level atas (yang bertanggung jawab jika terjadi insiden).
4. Dipantau hingga risiko tersebut dapat diperbaiki.

2.4 Konsep Ketahanan (Resilience) dan Disaster Recovery Center

Dalam kerangka kerja keamanan informasi C-I-A-A (Confidentiality, Integrity, Availability, Accountability) yang dijelaskan Wheeler (2011: 10), konsep *Disaster Recovery* berkaitan erat dengan pilar **Availability (Ketersediaan)**.

2.4.1 Konsep Dasar *Resilience*

Wheeler (2011: 140) mendefinisikan ketahanan (*resilience*) sebagai kemampuan sumber daya untuk bertahan dari gangguan. Gangguan ini bisa berupa serangan siber, kegagalan infrastruktur, atau bencana alam. Dalam konteks regulasi TI, organisasi dituntut untuk menjamin ketersediaan layanan kritis (*critical services*).

Disaster Recovery Center (DRC) adalah implementasi fisik dan logikal dari konsep ketahanan ini. DRC bukan sekadar "tempat cadangan", melainkan sebuah strategi arsitektur yang memastikan bahwa fungsi bisnis tetap berjalan atau dapat pulih dengan cepat setelah kejadian destruktif.

2.4.2 Strategi dan Arsitektur *Disaster Recovery*

Wheeler membagi strategi pemulihan dan ketahanan menjadi dua komponen utama:

1. **Ketahanan Fisik (*Physical Resilience*):**

   Melibatkan redundansi pada level infrastruktur fisik. Ini mencakup:

   - **Site Redundancy:** Memiliki lokasi alternatif (DRC) yang terpisah secara geografis dari pusat data utama. Hal ini memitigasi risiko bencana alam (banjir, gempa) yang mungkin melumpuhkan satu lokasi spesifik.
   - **Hardware Redundancy:** Penyediaan perangkat keras cadangan di DRC yang siap mengambil alih beban kerja.

2. **Ketahanan Logikal (*Logical Resilience*):**

   Melibatkan desain sistem dan aplikasi untuk mendukung pemulihan.

   - **High Availability (HA) Configurations:** Konfigurasi sistem di mana layanan dapat berpindah (*failover*) secara otomatis ke sistem di DRC tanpa gangguan yang berarti bagi pengguna.
   - **Stateful Failover:** Kemampuan perangkat kontrol (seperti *firewall* di DRC) untuk mengambil alih koneksi aktif tanpa mengharuskan pengguna melakukan *login* ulang.

Wheeler secara spesifik menyebutkan persyaratan untuk *"Comply with standards for Distributed Computing High Availability"* dan *"Manage capacity and redundancy"* sebagai kontrol teknologi yang harus ada untuk memitigasi risiko ketersediaan.

2.4.3 Evaluasi Kelangsungan Bisnis Pihak Ketiga

Konsep DRC juga sangat krusial ketika organisasi menggunakan layanan pihak ketiga. Wheeler (2011) membahas penggunaan kuesioner **SIG (Standardized Information Gathering)**.

Kuesioner **SIG-K: Business Continuity and Disaster Recovery** (Wheeler, 2011: 208) digunakan untuk mengevaluasi apakah vendor memiliki DRC yang memadai. Mahasiswa dan praktisi harus memahami bahwa tanggung jawab atas ketersediaan data tidak hilang saat data tersebut disimpan di *cloud* atau vendor; organisasi harus memastikan (melalui audit atau kuesioner) bahwa penyedia layanan memiliki fasilitas DRC yang teruji secara berkala.

BAB III
KESIMPULAN

3.1 Kesimpulan

Berdasarkan pembahasan mengenai proses pencapaian dan pemeliharaan kepatuhan terhadap regulasi TI dengan mengacu pada pustaka *Wheeler, E. (2011). Security Risk Management*, dapat ditarik beberapa kesimpulan utama sebagai berikut:

1. **Pergeseran Paradigma Kepatuhan:**

   Pencapaian kepatuhan terhadap regulasi TI tidak dapat lagi dipandang sebagai aktivitas "daftar periksa" (*checklist*) sesaat. Wheeler menegaskan bahwa kepatuhan adalah hasil alami dari program manajemen risiko yang matang. Implementasi *Security Risk Reviews* (SRR) dan *Gap Analysis* menjadi metode fundamental untuk mengidentifikasi perbedaan antara standar regulasi dengan realitas operasional. Pemeliharaan kepatuhan menuntut penerapan siklus hidup yang berkelanjutan (*continuous monitoring*) sebagaimana diadopsi dalam kerangka kerja NIST, di mana setiap perubahan pada lingkungan TI memicu evaluasi ulang risiko.

2. **Integrasi Etika dan Privasi dalam Profil Risiko:**

   Manajemen risiko TI memiliki dimensi etika yang krusial. Prinsip *"Safety before Security"* harus menjadi landasan utama, di mana kontrol keamanan tidak boleh membahayakan keselamatan fisik atau hak dasar manusia. Dalam konteks perlindungan data pribadi, proses *risk profiling* harus secara eksplisit menilai sensitivitas informasi (*Personally Identifiable Information*) untuk menentukan kewajiban etis organisasi. Kepatuhan bukan hanya tentang menghindari denda regulasi, tetapi juga memenuhi kontrak sosial untuk menjaga privasi pengguna agar tidak terjadi penyalahgunaan data atau pemantauan yang berlebihan (*over-surveillance*).

3. **Dampak Strategis terhadap Pemangku Kepentingan (*Stakeholders*):**
   Setiap keputusan manajemen risiko baik itu mitigasi, transfer, atau penerimaan risiko memiliki konsekuensi langsung terhadap berbagai pemangku kepentingan. Tim keamanan berperan sebagai penasihat (*advisor*) yang memfasilitasi pengambilan keputusan dengan menerjemahkan risiko teknis ke dalam dampak bisnis (finansial, reputasi, dan legal). Mekanisme formal seperti manajemen pengecualian (*exception management*) sangat penting untuk memastikan transparansi dan akuntabilitas, sehingga para eksekutif bisnis sadar penuh akan risiko yang mereka ambil atas nama organisasi.
4. **Ketahanan Sistem Melalui *Disaster Recovery Center* (DRC):**
   Dalam pilar ketersediaan (*availability*) pada model C-I-A-A, konsep *Disaster Recovery Center* (DRC) merupakan komponen vital dari arsitektur ketahanan (*resilience*). DRC bukan sekadar fasilitas cadangan teknis, melainkan strategi manajemen risiko untuk menjamin kelangsungan layanan kritis saat terjadi gangguan besar. Implementasi DRC mencakup redundansi fisik (*site redundancy*) dan logikal (*high availability*) yang harus divalidasi efektivitasnya, baik untuk infrastruktur internal maupun penyedia layanan pihak ketiga (vendor).

3.2 Saran

Berdasarkan analisis materi dari buku *Security Risk Management*, penulis mengajukan beberapa saran praktis bagi organisasi maupun praktisi TI:

1. **Adopsi Pendekatan Berbasis Risiko, Bukan Hanya Kepatuhan:**
   Organisasi disarankan untuk tidak hanya fokus memenuhi butir-butir regulasi secara kaku. Sebaliknya, gunakan metodologi *Security Risk Reviews* untuk menyesuaikan kontrol keamanan dengan profil risiko spesifik organisasi. Jika sebuah kontrol regulasi tidak dapat diterapkan, gunakan proses pengecualian formal yang didukung oleh kontrol kompensasi yang memadai.

2. **Formalisasi Tinjauan Etika dalam Penilaian Risiko:**

   Disarankan agar formulir penilaian risiko (seperti kuesioner profil risiko) memasukkan pertanyaan eksplisit mengenai dampak keselamatan manusia dan privasi pengguna. Hal ini untuk mencegah penerapan kontrol keamanan yang intrusif atau pengabaian terhadap perlindungan data sensitif.

3. **Peningkatan Komunikasi Risiko kepada Eksekutif:**

   Praktisi keamanan harus menghindari penggunaan jargon teknis saat melaporkan status kepatuhan kepada pemangku kepentingan. Laporan risiko harus dikonversi ke dalam metrik dampak bisnis (misalnya: potensi kerugian finansial atau dampak reputasi merek) agar mendapatkan dukungan dan alokasi sumber daya yang tepat.

4. **Validasi Berkala terhadap *Disaster Recovery Plan*:**

   Memiliki DRC saja tidak cukup. Organisasi harus melakukan pengujian berkala (seperti simulasi *failover*) untuk memastikan integritas data dan waktu pemulihan (*Recovery Time Objective*) sesuai dengan standar regulasi. Selain itu, evaluasi terhadap vendor pihak ketiga menggunakan standar seperti SIG (Standardized Information Gathering) harus dilakukan untuk memastikan rantai pasok layanan juga memiliki ketahanan bencana yang memadai.

DAFTAR PUSTAKA

Wheeler, E. (2011). Building a Program from Scratch. In Security Risk Management. https://doi.org/10.1016/b978-1-59749-615-5.00014-1