Laporan Audit Internal Keamanan Siber

Perusahaan: Botium Toys
Tanggal Audit: 5 September 2025
Pemeriksa: Tegar Pramudya

Skenario

Botium Toys adalah bisnis kecil di AS yang mengembangkan dan menjual mainan. Bisnis ini memiliki satu lokasi fisik, yang berfungsi sebagai kantor pusat, etalase, dan gudang untuk produk-produk mereka. Namun, kehadiran daring Botium Toy telah berkembang pesat, menarik pelanggan di AS dan luar negeri. Akibatnya, departemen teknologi informasi (TI) mereka berada di bawah tekanan yang semakin besar untuk mendukung pasar daring mereka di seluruh dunia.

Manajer departemen TI telah memutuskan bahwa audit TI internal perlu dilakukan. Ia khawatir tentang kepatuhan dan operasional bisnis seiring pertumbuhan perusahaan tanpa rencana yang jelas. Ia yakin audit internal dapat membantu mengamankan infrastruktur perusahaan dengan lebih baik dan membantu mereka mengidentifikasi serta memitigasi potensi risiko, ancaman, atau kerentanan terhadap aset-aset penting. Manajer juga berkepentingan untuk memastikan bahwa mereka mematuhi peraturan terkait pemrosesan dan penerimaan pembayaran daring internal serta menjalankan bisnis di Uni Eropa (UE).

Manajer TI memulai dengan menerapkan Kerangka Kerja Keamanan Siber dari Institut Nasional Standar dan Teknologi (NIST CSF), menetapkan ruang lingkup dan tujuan audit, mencantumkan aset yang saat ini dikelola oleh departemen TI, dan

menyelesaikan penilaian risiko. Tujuan audit adalah untuk memberikan gambaran umum tentang risiko dan/atau denda yang mungkin dialami perusahaan akibat kondisi keamanan mereka saat ini.

Tugas Anda adalah meninjau cakupan, tujuan, dan laporan penilaian risiko manajer TI. Kemudian, lakukan audit internal dengan melengkapi daftar periksa kontrol dan kepatuhan.

Botium Toys: Cakupan, tujuan, dan laporan penilaian risiko

Ruang lingkup dan tujuan audit

Ruang lingkup: Cakupan audit ini mencakup keseluruhan program keamanan di Botium Toys. Ini mencakup aset mereka seperti peralatan dan perangkat karyawan, jaringan internal, dan sistem mereka. Anda perlu meninjau aset yang dimiliki Botium Toys serta kontrol dan praktik kepatuhan yang mereka terapkan.

Sasaran: Menilai aset yang ada dan menyelesaikan daftar periksa kontrol dan kepatuhan untuk menentukan kontrol dan praktik terbaik kepatuhan mana yang perlu diterapkan untuk meningkatkan postur keamanan Botium Toys.

Aset lancar

Aset yang dikelola oleh Departemen TI meliputi:

- Peralatan di tempat untuk kebutuhan bisnis di kantor
- Peralatan karyawan: perangkat pengguna akhir (desktop/laptop, telepon pintar), stasiun kerja jarak jauh, headset, kabel, keyboard, mouse, stasiun dok, kamera pengintai, dll.
- Produk etalase tersedia untuk dijual eceran di lokasi dan online; disimpan di gudang perusahaan yang bersebelahan
- Manajemen sistem, perangkat lunak, dan layanan: akuntansi, telekomunikasi, basis data, keamanan, e-commerce, dan manajemen inventaris
- Akses internet
- Jaringan internal
- Retensi dan penyimpanan data
- Pemeliharaan sistem lama: sistem akhir masa pakai yang memerlukan pemantauan manusia

Penilaian risiko

Deskripsi risiko

Saat ini, pengelolaan aset masih belum memadai. Botium Toys juga belum memiliki semua kontrol yang memadai dan mungkin belum sepenuhnya mematuhi peraturan dan standar AS dan internasional.

Kontrol praktik terbaik

Fungsi pertama dari lima fungsi NIST CSF adalah Identifikasi. Botium Toys perlu mengalokasikan sumber daya untuk mengidentifikasi aset agar dapat mengelolanya dengan tepat. Selain itu, mereka perlu mengklasifikasikan aset yang ada dan menentukan dampak hilangnya aset yang ada, termasuk sistem, terhadap kelangsungan bisnis.

Skor risiko

Pada skala 1 sampai 10, skor risikonya adalah 8, yang cukup tinggi. Hal ini disebabkan oleh kurangnya kontrol dan kepatuhan terhadap praktik terbaik kepatuhan.

Komentar tambahan

Potensi dampak dari hilangnya aset dinilai sedang, karena departemen TI tidak mengetahui aset mana yang berisiko. Risiko terhadap aset atau denda dari badan pengatur tinggi karena Botium Toys tidak memiliki semua kontrol yang diperlukan dan tidak sepenuhnya mematuhi praktik terbaik terkait peraturan kepatuhan yang menjaga privasi/keamanan data penting. Tinjau poin-poin berikut untuk detail spesifik:

- Saat ini, semua karyawan Botium Toys memiliki akses ke data yang disimpan secara internal dan mungkin dapat mengakses data pemegang kartu dan PII/SPII pelanggan.
- Enkripsi saat ini tidak digunakan untuk memastikan kerahasiaan informasi kartu kredit pelanggan yang diterima, diproses, dikirimkan, dan disimpan secara lokal di basis data internal perusahaan.
- Kontrol akses yang berkaitan dengan hak istimewa paling rendah dan pemisahan tugas belum diterapkan.
- Departemen TI telah memastikan ketersediaan dan kontrol terintegrasi untuk memastikan integritas data.
- Departemen TI memiliki firewall yang memblokir lalu lintas berdasarkan serangkaian aturan keamanan yang ditetapkan dengan tepat.

- Perangkat lunak antivirus dipasang dan dipantau secara berkala oleh departemen TI.
- Departemen TI belum memasang sistem deteksi intrusi (IDS).
- Tidak ada rencana pemulihan bencana yang diterapkan saat ini, dan perusahaan tidak memiliki cadangan data penting.
- Departemen TI telah menetapkan rencana untuk memberi tahu pelanggan Uni Eropa dalam waktu 72 jam jika terjadi pelanggaran keamanan. Selain itu, kebijakan, prosedur, dan proses privasi telah dikembangkan dan ditegakkan di antara anggota departemen TI/karyawan lainnya, untuk mendokumentasikan dan memelihara data dengan baik.
- Meskipun ada kebijakan kata sandi, persyaratannya bersifat nominal dan tidak sejalan dengan persyaratan kompleksitas kata sandi minimum saat ini (misalnya, minimal delapan karakter, kombinasi huruf dan minimal satu angka; karakter khusus).
- Tidak ada sistem manajemen kata sandi terpusat yang menerapkan persyaratan minimum kebijakan kata sandi, yang terkadang memengaruhi produktivitas saat karyawan/vendor mengirimkan tiket ke departemen TI untuk memulihkan atau mengatur ulang kata sandi.
- Meskipun sistem lama dipantau dan dipelihara, tidak ada jadwal rutin untuk tugas-tugas ini dan metode intervensi tidak jelas.
- Lokasi fisik toko, yang meliputi kantor utama Botium Toys, bagian depan toko, dan gudang produk, memiliki kunci yang memadai, pengawasan televisi sirkuit tertutup (CCTV) terkini, serta sistem deteksi dan pencegahan kebakaran yang berfungsi.

Daftar Periksa Kontrol dan Kepatuhan

Pilih “ya” atau “tidak” untuk menjawab pertanyaan:*Apakah Botium Toys saat ini memiliki kontrol ini?*

Daftar periksa penilaian kontrol

Ya	TIDAK	Kontrol	*Penjelasan*
☐	☑	Hak Istimewa Paling Rendah	Semua karyawan Botium Toys memiliki akses ke data yang disimpan secara internal sehingga memungkinkan mereka untuk dapat mengakses data pemegang kartu dan PII/SPII pelanggan.
☐	☑	Rencana pemulihan bencana	Botium Toys belum memiliki rencana pemulihan bencana. Oleh karena itu, Botuna Toys harus segera merencakan dan menyusun rancangan mengenai hal tersebut.
☐	☑	Kebijakan kata sandi	Botium Toys sudah menerapkan kebijakan kata sandi namun masih bersifat nominal dan tidak sesuaik dengan persyaratan kompleksitas kata sandi minimum secara umum (minimal 8 karakter, kombinasi huruf dan minimal satu, serta satu karakter khusus). Oleh

			karena itu, Botium Toys perlu menerapkan kebijakan kata sandi yang sesuai secepatnya.
☐	☑	Pemisahan tugas	Perlu diterapkan untuk mengurangi kemungkinan penipuan/akses ke data penting, karena CEO perusahaan saat ini menjalankan operasi sehari-hari dan mengelola penggajian.
☑	☐	Tembok api	Firewall sudah ada dan diterapkan oleh departemen IT Botium Toys. Firewall ini bertugas untuk memblokir lalu lintas berdasarkan serangkaian aturan keamanan yang ditetapkan dengan tepat
☐	☑	Sistem deteksi intrusi (IDS)	Departemen TI Botium Toys memerlukan pemasangan IDS agar segala jenis kemungkinan ancaman oleh aktor kejahatan dapat diidentifikasi.
☐	☑	Cadangan	Departemen IT Botium Toys memerlukan cadangan yang berisikan data penting perusahaan untuk meminimalkan dampak berkelanjutan perusahaan jika pelanggaran dalam suatu waktu akan terjadi.
☑	☐	Perangkat lunak antivirus	Perangkat lunak antivirus dipasang dan dipantau secara berkala oleh departemen TI.
☐	☑	Pemantauan, pemeliharaan, dan intervensi manual untuk	Daftar aset mencatat penggunaan sistem lama.

		sistem lama	Penilaian risiko menunjukkan bahwa sistem ini dipantau dan dipelihara, tetapi tidak ada jadwal rutin untuk tugas ini dan prosedur/kebijakan terkait intervensi tidak jelas, yang dapat menempatkan sistem ini pada risiko pelanggaran.
☐	☑	Enkripsi	Tidak ada penerapan enkripsi pada perusahaan Botium Toys. Enkripsi diperlukan agar kerahasiaan informasi kartu kredit pelanggan yang diterima, diproses, dikirimkan, dan disimpan dalam sistem jaringan lokal atau dibasis data internal perusahaan bisa dipastikan dan diamankan dengan lebih baik.
☐	☑	Sistem manajemen kata sandi	Saat ini tidak ada sistem manajemen kata sandi; penerapan kontrol ini akan meningkatkan produktivitas departemen TI/karyawan lain jika terjadi masalah kata sandi.
☑	☐	Kunci (kantor, etalase, gudang)	Lokasi fisik toko yang terdiri dari kantor utama Botium Toys, bagian depan toko, dan gudang produk sudah memiliki kunci yang memadai, kamera pengawas (CCTV) terbaru, serta sistem deteksi dan pencegahan kebakaran yang berfungsi.
☑	☐	Pengawasan televisi sirkuit tertutup (CCTV)	CCTV sudah dipasang/berfungsi di lokasi fisik toko.
☑	☐	Deteksi/pencegahan	Lokasi fisik Botium Toys

	kebakaran (alarm kebakaran, sistem sprinkler, dll.)	memiliki sistem deteksi dan pencegahan kebakaran yang berfungsi.

Daftar periksa kepatuhan

Pilih “ya” atau “tidak” untuk menjawab pertanyaan:*Apakah Botium Toys saat ini mematuhi praktik terbaik kepatuhan ini?*

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)

Ya	TIDAK	Praktik terbaik	*Penjelasan*
☐	☑	Hanya pengguna yang berwenang yang memiliki akses ke informasi kartu kredit pelanggan.	Semua karyawan Botium Toys dapat mengakses data kartu kredit pelanggan.
☐	☑	Informasi kartu kredit diterima, diproses, dikirimkan, dan disimpan secara internal, dalam lingkungan yang aman.	Informasi kartu kredit yang diterima, diproses, dikirimkan dan disimpan secara internal tidak di simpan dilingkungan yang aman. Hal ini dikarenakan data-data tersebut tidak dienkripsi.
☐	☑	Terapkan prosedur enkripsi data untuk mengamankan titik sentuh dan data transaksi kartu kredit dengan lebih baik.	Perusahaan saat ini tidak menggunakan enkripsi untuk lebih menjamin kerahasiaan informasi keuangan pelanggan.
☐	☑	Terapkan kebijakan manajemen kata sandi yang aman.	Kebijakan kata sandi bersifat nominal dan saat ini tidak ada sistem manajemen kata sandi yang diterapkan.

Peraturan Perlindungan Data Umum (GDPR)

Ya	TIDAK	Praktik terbaik	*Penjelasan*
☐	☑	Data pelanggan Uni Eropa dijaga privasinya/keamanannya.	Perusahaan saat ini tidak menggunakan enkripsi untuk lebih menjamin kerahasiaan informasi keuangan pelanggan.
☑	☐	Ada rencana untuk memberi tahu pelanggan UE dalam waktu 72 jam jika data mereka disusupi/terjadi pelanggaran.	Ada rencana untuk memberi tahu pelanggan UE dalam waktu 72 jam setelah terjadi pelanggaran data.
☐	☑	Pastikan data diklasifikasikan dan diinventarisasi dengan benar.	Aset lancar telah diinventarisasi/didaftarkan, tetapi belum diklasifikasikan.
☑	☐	Terapkan kebijakan, prosedur, dan proses privasi untuk mendokumentasikan dan memelihara data dengan benar.	Kebijakan, prosedur, dan proses privasi telah dikembangkan dan ditegakkan di antara anggota tim TI dan karyawan lainnya, sesuai kebutuhan.

Kontrol Sistem dan Organisasi (SOC tipe 1, SOC tipe 2)

Ya	TIDAK	Praktik terbaik	*Penjelasan*
☐	☑	Kebijakan akses pengguna ditetapkan.	Prinsip kontrol hak istimewa terendah dan pemisahan tugas belum diterapkan di Botium Toys. Hal ini dibuktikan dengan kerangan bahwa semua karyawan memiliki akses ke data yang disimpan secara internal.

☐	☑	Data sensitif (PII/SPII) bersifat rahasia/pribadi.	Kerahasiaan masih diragukan, dikarenakan data PII/SPII. yang ada di Botium Toys tidak dienkripsi sehingga masih mudah untuk dieksploitasi.
☑	☐	Integritas data memastikan data konsisten, lengkap, akurat, dan telah divalidasi.	Integritas data terjamin,seperti tidak berubah-ubah, lengkap, akurat dan telah divalidasi.
☐	☑	Data tersedia bagi individu yang berwenang untuk mengaksesnya.	Meskipun data tersedia untuk semua karyawan, otorisasi perlu dibatasi hanya pada individu yang memerlukan akses untuk melakukan pekerjaan mereka.

Rekomendasi (opsional):

Terdapat berbagai macam rekomendasi untuk Botuna Toys agar mengurangi nilai kerentanan akibat lemahnya kontrol akses, tidak diberlakukannya enktripsi, proses backup data penting belum diterapkan, hingga belum adanya perancanaan mengenai pemulihan bencana. Berikut merupakan poin-poin penting rekomendasi yang harus diperbaiki dan ditekankan oleh Botium Toys untuk mencapai keadaan keamanan siber yang memadai.

1. Kontrol Akses & Hak Istimewa

- Terapkan Prinsip Least Privilege (POLP) agar tidak semua karyawan memiliki akses ke data sensitif.
- Implementasikan Role-Based Access Control (RBAC) untuk membatasi akses hanya kepada karyawan yang relevan dengan pekerjaannya.
- Terapkan pemisahan tugas (Segregation of Duties) untuk mengurangi risiko penyalahgunaan wewenang, khususnya di area keuangan dan penggajian.

2. Manajemen Identitas & Kata Sandi

- Perbarui kebijakan kata sandi agar sesuai standar industri (≥ 12 karakter, kombinasi huruf besar, huruf kecil, angka, dan simbol).

- Terapkan sistem manajemen kata sandi terpusat yang mendukung MFA (Multi-Factor Authentication).

- Gunakan Single Sign-On (SSO) atau Identity Provider untuk meningkatkan keamanan sekaligus produktivitas.

3. Enkripsi & Proteksi Data

- Terapkan enkripsi end-to-end pada data sensitif, khususnya informasi kartu kredit dan PII/SPII.

- Gunakan standar enkripsi modern (AES-256, TLS 1.3 untuk komunikasi).

- Pastikan data at-rest dan data in-transit terlindungi.

4. Cadangan & Pemulihan Bencana (BCP/DRP)

- Buat rencana pemulihan bencana (Disaster Recovery Plan) lengkap dengan simulasi berkala.

- Terapkan backup otomatis & terenkripsi untuk data penting.

- Simpan cadangan di lokasi berbeda (off-site backup atau cloud backup).

5. Perlindungan Infrastruktur Jaringan

- Lanjutkan penggunaan firewall, tetapi perlu ditambah dengan:

- Intrusion Detection System (IDS) atau lebih baik lagi Intrusion Prevention System (IPS).

- SIEM (Security Information and Event Management) untuk monitoring real-time.

- Segmentasikan jaringan antara sistem internal, publik, dan sensitif (contoh: VLAN terpisah).

6. Manajemen Sistem Lama

- Buat jadwal pemeliharaan rutin untuk sistem perusahaan.

- Evaluasi apakah sistem lama masih layak dipertahankan atau perlu migrasi ke sistem yang lebih modern.
- Terapkan patch management agar sistem tidak memiliki celah keamanan yang sudah diketahui.

7. Kepatuhan Regulasi (PCI DSS, GDPR, SOC)

- PCI DSS:
    1. Batasi akses data kartu kredit hanya untuk staf berwenang.
    2. Terapkan enkripsi di semua tahap transaksi.
- GDPR:
    1. Pastikan data pelanggan UE dienkripsi & diklasifikasikan.
    2. Tegakkan prosedur pelaporan insiden 72 jam.
- SOC 2:
    - Perkuat kontrol akses, enkripsi, dan audit log.
    - Dokumentasikan semua prosedur agar siap jika ada audit eksternal.

8. Pelatihan & Kesadaran Keamanan

- Lakukan pelatihan keamanan siber rutin bagi semua karyawan.
- Terapkan simulasi phishing untuk mengurangi risiko serangan berbasis rekayasa sosial.
- Buat SOP keamanan data yang mudah dipahami karyawan non-TI.