Microsoft 365 Copilot

Kit Sprint Risiko AI Bayangan

Daftar periksa informasi umum dan perencana tindakan untuk membantu pemimpin keamanan dan TI mendiskusikan potensi penggunaan AI tanpa izin, risiko berbagi data yang berlebihan, pertimbangan perlindungan data, serta diskusi tata kelola bersama pemangku kepentingan internal yang relevan.



Ikhtisar

Kit Sprint Risiko AI Bayangan adalah kerangka informasi umum yang dirancang untuk mendukung percakapan terstruktur tentang potensi penggunaan AI tanpa izin, pertimbangan penanganan data, dan pendekatan tata kelola. Aset ini dimaksudkan untuk membantu tim mendiskusikan visibilitas, prioritas, dan koordinasi keputusan terkait AI di antara para pemangku kepentingan yang relevan.

Kit ini harus disesuaikan dengan lingkungan organisasi dan ditinjau berdasarkan dokumentasi Microsoft yang berlaku saat ini, lisensi, ketersediaan, serta persyaratan hukum, privasi, kepatuhan, keamanan, TI, pengadaan, dan bisnis yang relevan sebelum digunakan.

Daftar Isi

3
Kuis risiko AI bayangan

4
Peta sprint 5 hari

5
Perencana tindakan

6
Pelajari selengkapnyae

Saat yang tepat menggunakan sprint ini

Sprint ini dapat digunakan sebagai alat fasilitasi ketika aplikasi AI, kopilot, agen, atau ekstensi mungkin diadopsi dengan kecepatan yang berbeda dari proses peninjauan internal. Tujuan dari panduan ini adalah untuk mendukung diskusi dan penentuan prioritas, dan tidak menetapkan tindakan yang wajib dilakukan.

Hasil sprint yang disarankan

- Susun inventaris kerja untuk diskusi tentang alat AI dan titik kontak data.
- Identifikasi dan prioritaskan area yang perlu ditinjau lebih lanjut.
- Jelajahi potensi pertimbangan akses dan perlindungan data untuk ditinjau oleh pemangku kepentingan.
- Diskusikan pendekatan tata kelola yang mungkin, termasuk kepemilikan dan frekuensi pelaksanaannya.

Penafian

Konten ini disediakan hanya untuk tujuan informasi. Ini bukan merupakan nasihat hukum, peraturan, kepatuhan, maupun teknis dan tidak menjamin deteksi, perlindungan, pengurangan risiko, atau hasil kepatuhan. Organisasi bertanggung jawab untuk secara independen mengevaluasi kewajiban, toleransi risiko, dan konfigurasi teknis mereka, termasuk kemampuan produk, ketersediaan, dan lisensi.

Mulai di sini: kuis cepat risiko AI bayangan

Gunakan tanggapan sebagai masukan arahan untuk diskusi saja. Beberapa tanggapan dengan tingkat kekhawatiran yang lebih tinggi dapat menunjukkan topik yang memerlukan visibilitas tambahan, tinjauan pemangku kepentingan, atau prioritas. Beberapa tanggapan dengan tingkat kekhawatiran moderat dapat menyarankan area dengan kepemilikan, kejelasan kebijakan, atau rutinitas bukti dapat bermanfaat. Sebagian besar respons yang menunjukkan kekhawatiran rendah mungkin mengindikasikan bahwa sprint dapat digunakan sebagai diskusi kesiapan dan latihan optimalisasi.

Kuis ini bukanlah penilaian formal, metodologi penilaian, audit, atau penentuan kepatuhan, dan langkah selanjutnya harus mencerminkan konteks hukum, peraturan, kontrak, teknis, dan operasional masing-masing organisasi.

Pertanyaan diskusi	Tingkat kekhawatiran rendah	Kekhawatiran sedang	Kekhawatiran Tinggi
Apakah Anda memiliki gambaran terkini tentang aplikasi AI, ekstensi, kopilot, plugin, dan agen yang sedang digunakan?	□ Inventaris tampak terkini.	□ Visibilitas parsial.	□ Tidak ada tampilan yang dapat diandalkan.
Bisakah Anda melihat data sensitif apa yang mungkin diakses oleh perangkat AI?	□ Akses tampaknya sudah dipetakan.	□ Hanya alat inti.	□ Tidak diketahui atau tidak konsisten.
Apakah alat dan jalur AI yang disetujui sudah jelas?	□ Jalurnya tampak jelas.	□ Panduan tidak merata.	□ Tim memilih alat secara independen.
Apakah kontrol dipetakan ke jalur data yang terkait dengan AI?	□ Kontrol tampak dipetakan.	□ Beberapa alur kerja yang dibahas.	□ Tidak dipetakan untuk penggunaan AI.
Apakah ada bukti terkait keputusan tata kelola AI?	□ Pemilik dan irama tampak terdefinisi.	□ Bukti bersifat ad hoc.	□ Tidak ada jalur pembuktian yang konsisten.

Peta sprint lima hari

Gunakan tanggapan sebagai masukan arahan untuk diskusi saja. Beberapa tanggapan dengan tingkat kekhawatiran yang lebih tinggi dapat menunjukkan topik yang memerlukan visibilitas tambahan, tinjauan pemangku kepentingan, atau prioritas. Beberapa tanggapan dengan tingkat kekhawatiran moderat dapat menyarankan area dengan kepemilikan, kejelasan kebijakan, atau rutinitas bukti dapat bermanfaat. Sebagian besar respons yang menunjukkan kekhawatiran rendah mungkin mengindikasikan bahwa sprint dapat digunakan sebagai diskusi kesiapan dan latihan optimalisasi.

Kuis ini bukanlah penilaian formal, metodologi penilaian, audit, atau penentuan kepatuhan, dan langkah selanjutnya harus mencerminkan konteks hukum, peraturan, kontrak, teknis, dan operasional masing-masing organisasi.

Hari	Fokus	Tindakan	Output	Daftar periksa
1	Diskusikan potensi penggunaan AI tanpa izin.	Tinjau sinyal, pisahkan alat yang dikenal dari yang tidak dikenal, dan tangkap konteks bisnisnya.	Susun inventaris awal, buat daftar alat, dan tentukan pemilik tindak lanjut.	□ Sumber yang diidentifikasi □ Alat-alat yang tidak dikenal dicatat □ Kesenjangan dicatat
2	Diskusikan area tinjauan potensial.	Kelompokkan kasus penggunaan berdasarkan sensitivitas, akses, berbagi, otomatisasi, dan pertimbangan kepatuhan.	Inventaris diskusi yang diprioritaskan dan daftar tinjauan pemangku kepentingan.	□ Jalur data dicatat □ Alat-alat dengan risiko lebih tinggi diidentifikasi □ Pemilik yang disarankan
3	Lindungi data dan akses.	Diskusikan kontrol dasar, skenario perlindungan data, dan pertimbangan akses atau titik akhir.	Pertimbangan kontrol, poin-poin kebijakan, dan area pemantauan.	□ Kontrol yang dibahas □ DLP atau label dicatat □ Kesenjangan pemantauan dicatat
4	Atur aplikasi dan agen AI.	Buat draf kepemilikan, alur masuk, jalur pengecualian, dan kebutuhan bukti.	Peran, jalur peninjauan, dan konsep register bukti.	□ Pemilik telah diidentifikasi □ Pengecualian dicatat □ Pendaftaran dimulai
5	Jadikan sprint sebagai ritme yang berulang.	Konfirmasi prioritas, buat panduan, dan ajukan ritme 30 hari.	Prioritas perencanaan, garis besar panduan, topik pembacaan, dan ritme.	□ Prioritas didokumentasikan □ Pedoman disusun □ Ritme diusulkan

Peta perencana 30 hari tindakan

Rekomendasi laporan kepemimpinan. Contoh topik meliputi pola penggunaan AI, pertimbangan data, penentuan prioritas tindakan, keselarasan pemangku kepentingan, dan perencanaan dalam waktu dekat.

Prioritas	Pemilik	Tindakan	Bukti / sinyal keberhasilan	Jatuh tempo
1				
2				
3				
4				
5				
6				

Pelajari selengkapnya dari Microsoft

Jelajahi sumber daya Microsoft Security tentang pengamanan dan tata kelola penggunaan AI, termasuk panduan untuk perlindungan data, identitas dan akses, keamanan titik akhir, serta adopsi AI yang bertanggung jawab.

Cegah risiko agar Anda dapat bergerak maju dengan aman menggunakan Microsoft Security
Jelajahi Transformasi Frontier—tempat kecerdasan dan kepercayaan dengan Microsoft AI
AI yang aman dan keamanan data untuk produktivitas dengan Microsoft 365

