چارچوب حسابرسی

هوش مصنوعی

انجمن حسابرسان داخلی IIA

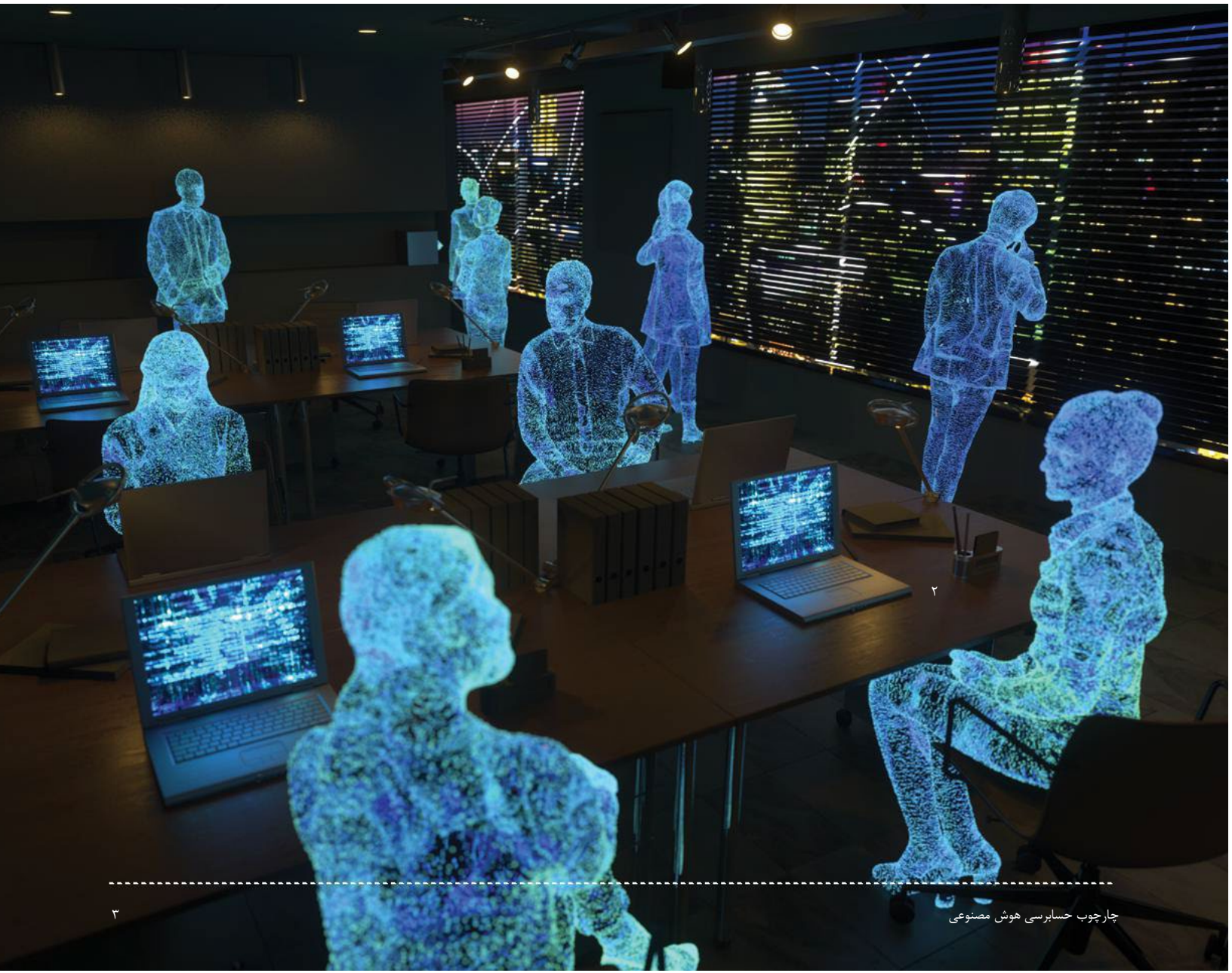
برگردان به فارسی:

مرتضی اسدی ساناز حجی

فروردین ۱۴۰۴

The Institute of
Internal Auditors

فهرست مطالب



مقدمه

هوش مصنوعی (AI) یک اصطلاح گسترده است که برای در بر گرفتن طیف وسیعی از فناوریهای موجود و نوظهور، ساخته شده است. اگرچه تعریف واحد و مورد توافقی برای آن وجود ندارد، اما هوش مصنوعی به طور کلی به "سیستم‌هایی اطلاق می‌شود که دارای فرآیندهای فکریِ با مشخصه انسان هستند، مانند توانایی استدلال، کشف معنا، تعمیم دادن یا یادگیری از تجربه‌های گذشته"[1]. رونق کنونی برنامه‌های کاربردی هوش مصنوعی، راه‌های به‌ظاهر بی‌پایانی را نشان می‌دهد که سازمان‌ها می‌توانند از فناوریهای مبتنی بر هوش مصنوعی برای بهبود روش کار خود استفاده کنند، در حالی که ریسک‌های متعدد و مهمی را ایجاد می‌کند که با توجه به ماهیت این فناوری، ذاتی هستند.

هوش مصنوعی می‌تواند موضوعی دلهره‌آور برای یک حسابرس داخلی باشد، به ویژه با توجه به اینکه پذیرش و استفاده از هوش مصنوعی در سازمان‌ها کماکان در حال افزایش است. اکنون بیش از هر زمان دیگری، سازمان‌ها برای راهنمایی بیشتر در مورد هوش مصنوعی به حسابرسی داخلی چشم دوخته‌اند. چه به عنوان مشاور در مورد ریسک‌ها و کنترل‌های مرتبط با هوش مصنوعی و چه در نقش اطمینان‌بخشی در مورد فرآیندهایی که از هوش مصنوعی استفاده می‌کنند یا به آن متکی هستند، ضروری است که حسابرسان داخلی دانش خود را در مورد موضوع هوش مصنوعی افزایش دهند.

از حسابرسان داخلی انتظار می‌رود که فعالیت‌های اطمینان‌بخشی را پیرامون فرآیندهایی ارائه دهند که می‌توانند از تراکنش‌های تجاری ساده تا رویه‌های بسیار پیچیده که نیاز به درک عمیق دارند، متغیر باشند. گستره و عمق سواد هوش مصنوعی مورد نیاز برای پشتیبانی از فعالیت‌های اطمینان‌بخشی، چالش‌های مستمری را برای حسابرسان داخلی ایجاد می‌کند که باید به طور مداوم دانش خود را از هوش مصنوعی توسعه دهند تا به طور کامل ریسک‌ها و عملکرد آن را درک کرده و مشاوره و اطمینان‌بخشی آگاهانه ارائه دهند

هوش مصنوعی به عنوان یک موضوع حسابرسی، چالش‌های منحصر به فرد خود را دارد و تکامل آن به این معنی است که حسابرسان داخلی باید ریسک و کاهش ریسک را در محیط هوش مصنوعی مجدداً ارزیابی کنند.

حال، حسابرسان داخلی از قبل مهارت‌های اساسی مهمی مانند تفکر انتقادی، ترسیم فرآیندها، ارزیابی ریسک، ارزیابی کنترل‌های فناوری اطلاعات، شناخت استراتژی‌های سازمانی و ارائه اطمینان‌بخشی مستقل به عملکرد ارکان راهبری را دارا هستند.

هدف از چارچوب حسابرسی هوش مصنوعی انجمن حسابرسان داخلی (IIA) کمک به حسابرسان داخلی در شناخت ریسک و تشخیص بهترین شیوه‌ها و کنترل‌های داخلی برای هوش مصنوعی است. این چارچوب به حسابرسان داخلی در توسعه دانش پایه کمک خواهد کرد. این چارچوب در چهار بخش ارائه شده است:

۱. مرور کلی – تاریخچه و کاربردهای هوش مصنوعی.

۲.آغاز به کار – شناخت اینکه یک سازمان چگونه از هوش مصنوعی استفاده می‌کند.

۳.چارچوب حسابرسی هوش مصنوعی – راهبری، مدیریت و حسابرسی داخلی.

۴.راهنمای فعالان و واژه‌نامه.

این چارچوب، که از جنبه‌های مدل سه خطی IIA [2] بهره می‌برد، شامل ارجاعاتی به چارچوب بین‌المللی اجرای حرفه‌ای (IPPF) خواهد بود که مبنایی برای الزامات اجباری و اصول راهنما برای حرفه حسابرسی داخلی ارائه می‌دهد. استانداردهای قابل اجرا باید برای اطلاعات بیشتر بررسی شوند. راهنمایی‌های مرتبط IIA، مانند راهنمای‌های حسابرسی فناوری جهانی (GTAGs)، برای ارائه محتوای خاص موضوعی ارجاع داده شده‌اند. سایر چارچوب‌های مرتبط، مانند چارچوب مدیریت ریسک هوش مصنوعی NIST (AI RMF 1.0)، به عنوان منابع اضافی برای فعالان حسابرسی داخلی فهرست شده‌اند.

بخش اول

مرور کلی

تاریخچه و تحولات

به عنوان مرور کلی بر این موضوع، برای حسابرسان داخلی مهم است که شناخت درستی از توسعه تاریخی هوش مصنوعی، نحوه استفاده فعلی از هوش مصنوعی در صنایع مختلف و روندهای نوظهور هوش مصنوعی که حسابرسان داخلی باید در نظر بگیرند، داشته باشند.

ایده هوش مصنوعی به سال ۱۹۵۰ برمی‌گردد، زمانی که آلن تورینگ، ریاضی‌دان بریتانیایی، در مقاله خود با عنوان "ماشین‌های محاسباتی و هوش" این سوال را مطرح کرد: "آیا ماشین‌ها می‌توانند فکر کنند؟"[۳] او به عنوان یکی از بنیانگذاران هوش مصنوعی در پیشنهاد اینکه ماشین‌ها در نهایت قادر به باهوشی شبیه به انسان خواهند بود، در نظر گرفته می‌شود. دو سال بعد، آرتور لی ساموئل، دانشمند علوم کامپیوتر آمریکایی در IBM، برنامه‌ای را ایجاد کرد که می‌توانست با استفاده از مقادیر برنامه‌ریزی‌شده برای تشخیص بهترین حرکت، بازی چکرز را انجام دهد. پروژه تحقیقاتی تابستانی دارتموث[۴] در مورد هوش مصنوعی در سال ۱۹۵۶ یکی از اولین کاربردهای اصطلاح هوش مصنوعی بود که به جان مک‌کارتی، دانشمند علوم کامپیوتر و شناختی آمریکایی نسبت داده می‌شود.[۵]

دهه ۱۹۶۰ شاهد پیشرفت‌های زیادی در هوش مصنوعی بود، از جمله استفاده از رباتیک، برنامه‌های حل مسئله و اولین برنامه کامپیوتری تعاملی (که همچنین به عنوان یک برنامه شناخت زبان طبیعی یا NLP شناخته می‌شود) به نام ELIZA، که توسط جوزف وایزنباوم، دانشمند علوم کامپیوتر و استاد آلمانی-آمریکایی توسعه یافت. ELIZA را می‌توان اولین "چت‌بات" در نظر گرفت که برای شبیه‌سازی مکالمه با یک کاربر انسانی طراحی شده است.[۶]

توسعه هوش مصنوعی در دهه ۱۹۷۰ شامل اولین ربات هوشمند به نام WABOT بود که توسط دانشکده علوم و مهندسی دانشگاه واسدا در توکیو ایجاد شد و همچنین ادامه کار بر روی NLPها توسط راج ردی،[۷،۸] دانشمند علوم کامپیوتر هندی-آمریکایی. پیشرفت‌ها در دهه ۱۹۸۰ شامل توسعه یک ون مرسدس بنز بدون راننده در سال ۱۹۸۶ تحت نظارت ارنست دیکمانس، رهبر آلمانی فناوری رانندگی خودران بود.[۹]

دهه ۱۹۹۰ شاهد پیشرفت‌هایی در فناوریهای مرتبط با هوش مصنوعی بود، از جمله نرم‌افزار تشخیص گفتار در ویندوز مایکروسافت . IBM هوش مصنوعی بسیار مؤثری مانند "Deep Blue" را توسعه داد که در سال ۱۹۹۷ زمانی که گری کاسپاروف، استاد بزرگ شطرنج را شکست داد، خبرساز شد.[۱۰]

در دهه ۲۰۰۰، هوش مصنوعی به بخشی از زندگی روزمره ما تبدیل شد، از جمله برنامه‌هایی مانند Alexa آمازون، Siri اپل و Google Assistant. سال ۲۰۲۳ سال افزایش پذیرش مدل‌های زبانی بزرگ (LLM) مانند ChatGPT بود که قابلیت‌های هوش مصنوعی را از پیش‌بینی صرف نتایج به انواع مختلف تولید محتوا ارتقا داده است.

سطوح پذیرش

بر اساس شاخص جهانی پذیرش هوش مصنوعی IBM در سال ۲۰۲۳، معادل ۴۲ درصد از شرکت‌های مورد بررسی، گزارش دادند که از هوش مصنوعی در تجارت خود استفاده می‌کنند و ۴۰ درصد دیگر گزارش دادند که در حال بررسی هوش مصنوعی هستند.[۱۱] گسترش مداوم هوش مصنوعی نشان می‌دهد که چرا حسابرسان داخلی باید اطمینان حاصل کنند.

که حسابرسان در حال گنجاندن ریسک‌های مربوط به هوش مصنوعی در برنامه‌ریزی حسابرسی‌های خود هستند. علاوه بر این، حسابرسان داخلی باید به طور مداوم دانش خود را در مورد هوش مصنوعی توسعه دهند. قسمت ۲، "آغاز به کار"، به بررسی عمیق‌تر ملاحظاتی می‌پردازد که یک حسابرس داخلی می‌تواند از آن‌ها برای تشخیص استفاده از هوش مصنوعی در سازمان خود استفاده کند.

همانطور که چشم‌انداز هوش مصنوعی به تکامل خود ادامه می‌دهد، روش‌های دسته‌بندی هوش مصنوعی نیز تغییر می‌کنند. در حالی که دیدگاه‌های مختلفی در مورد نحوه گروه‌بندی اشکال مختلف هوش مصنوعی وجود دارد، بخش زیر خلاصه‌ای مختصر از اشکال رایج هوش مصنوعی ارائه می‌دهد که یا هم اکنون در حال استفاده هستند (ماشین واکنش‌پذیر و حافظه محدود) یا صرفاً نظری (نظریه ذهن و خودآگاه).

از منظر عملکردی، IBM [۱۲] هوش مصنوعی را به چهار نوع دسته‌بندی می‌کند:

۱. هوش مصنوعی ماشین واکنش‌پذیر

۲.هوش مصنوعی با حافظه محدود

۳.هوش مصنوعی نظریه ذهن

۴.هوش مصنوعی خودآگاه

هوش مصنوعی ماشین واکنش‌پذیر

- هوش مصنوعی واکنش‌پذیر نوعی هوش مصنوعی بدون حافظه است که برای انجام وظایف تنها بر اساس ورودی یا آموزش انسانی طراحی شده است. این سیستم‌ها که گاهی اوقات به عنوان هوش مصنوعی باریک یا ضعیف شناخته می‌شوند، برای برنامه‌نویسی تولید شده توسط انسان که به ماشین دستور می‌دهد چگونه به تنهایی عمل کند، به "انسان در حلقه" متکی هستند. این برنامه‌نویسی معمولاً به عنوان "الگوریتم" یا مجموعه‌ای از محاسبات شناخته می‌شود که شامل جنبه‌هایی از علوم کامپیوتر و ریاضیات یا آمار است.

مثال :

- آبی عمیق IBM

- برخی از برنامه‌های یادگیری ماشین به عنوان هوش مصنوعی ماشین واکنش‌پذیر طبقه‌بندی می‌شوند. یادگیری ماشین اغلب مبتنی بر مدل‌های آماری است که داده‌ها را تجزیه و تحلیل می‌کنند و نتایج پیش‌بینی‌کننده را از داده‌های ورودی تولید می‌کنند. به عنوان مثال، یک خرده‌فروش آنلاین می‌تواند از هوش مصنوعی در برنامه تلفن همراه یا وب‌سایت خود استفاده کند که محصولات را بر اساس سابقه خرید مصرف‌کننده پیشنهاد می‌کند. سابقه خرید کاربر منفرد مجموعه داده‌ای است که خروجی را هدایت می‌کند، که متناسب با آن کاربر است.

استفاده ازهوش مصنوعی

نظرسنجی تجاری هوش مصنوعی PwC در سال ۲۰۲۲ (ایالات متحده) - تصمیم‌گیری پشتیبانی‌شده با هوش مصنوعی توسط ۷۴٪ از پاسخ‌دهندگان نظرسنجی رهبران فناوری، ۶۲٪ از رهبران عملیات و نگهداری، ۶۱٪ از رهبران تجربه مشتری و ۶۰٪ از رهبران استراتژی مورد استفاده قرار می‌گیرد.

- نظرسنجی نبض چشم‌انداز مدیرعامل جهانی EY در سال ۲۰۲۳ - ۹۹٪ از مدیران عامل مورد بررسی در حال انجام یا برنامه‌ریزی سرمایه‌گذاری‌های قابل توجه در هوش مصنوعی مولد هستند.
- وضعیت هوش مصنوعی McKinsey در سال ۲۰۲۳ - ۷۹ درصد از همه پاسخ‌دهندگان جهانی گزارش می‌دهند که تا حدی در معرض هوش مصنوعی مولد قرار گرفته‌اند و ۲۲ درصد گفته‌اند که به طور منظم از آن استفاده می‌کنند.

هوش مصنوعی با حافظه محدود

- هوش مصنوعی حافظه محدود وابستگی کمتری به تعامل انسانی برای تولید نتایج دارد و به آن توانایی منحصر به فردی برای یادگیری و بهبود بر اساس آموزش از مجموعه‌های داده بزرگتر می‌دهد. در حالی که هوش مصنوعی ماشین واکنش‌پذیر فقط می‌تواند از داده‌های موجود فعلی استفاده کند، هوش مصنوعی حافظه محدود می‌تواند داده‌های گذشته و حال را برای بهبود عملکرد در طیف وسیعی از ابزارهای جدید هوش مصنوعی ادغام کند.

- نمونه‌های دیگر یادگیری ماشین که به مجموعه‌های بسیار بزرگتری از داده‌ها دسترسی دارند و تجزیه و تحلیل پیچیده‌تری را انجام می‌دهند، به عنوان "یادگیری عمیق" شناخته می‌شود و زیرمجموعه‌ای از یادگیری ماشین و هوش مصنوعی حافظه محدود است. تفاوت آن در وابستگی کمتر به تعامل انسانی برای تولید نتایج است. هوش مصنوعی مولد در این دسته قرار می‌گیرد و می‌تواند برای ایجاد محتوا بر اساس الگوریتم‌های برنامه‌ریزی شده مورد استفاده قرار گیرد.

نمونه‌هایی از هوش مصنوعی مولد عبارتند از:

ChatGPT، LLaMA و Bard نمونه‌هایی از ربات‌های چت LLM هستند که به یادگیری عمیق متکی هستند و می‌توانند محتوای متنی تولید کنند، در حالی که اشکال دیگر هوش مصنوعی مولد می‌توانند محتوایی مانند موسیقی (MusicLM)، هنر (DALL-E) و حتی کدنویسی رایانه (OpenAI Codex) تولید کنند.

چت‌بات‌ها و دستیاران مجازی نوعی رایج از هوش مصنوعی حافظه محدود (Limited Memory AI) هستند که از پردازش زبان طبیعی (NLP) و یادگیری تقویتی برای تعامل در مکالمات شبیه به انسان با کاربران نهایی استفاده می‌کنند. این ابزارها اغلب توسط سازمان‌هایی مانند موسسات مالی مورد استفاده قرار می‌گیرند که به کاربر اجازه می‌دهند حتی خارج از ساعات کاری، مشکلات خود را برطرف کنند.

به علاوه، یادگیری ماشین اغلب به چهار دسته تقسیم می‌شود:[۱۳]

یادگیری نظارت‌شده – یادگیری گذشته بر روی داده‌های ساختاریافته با نتایج از پیش تعیین‌شده اعمال می‌شود.

یادگیری بدون نظارت – هیچ نتیجه "درست" از پیش تعیین‌شده‌ای وجود ندارد؛ بلکه به دنبال الگوها در داده‌های بدون ساختار است.

یادگیری نیمه‌نظارتی – شامل عناصری از هر دو یادگیری نظارت‌شده و بدون نظارت است.

یادگیری تقویت شده – برنامه‌نویسی پویا که در آن از طریق یک سیستم پاداش و تنبیه، آموزش داده می‌شوند. بدون تعامل انسانی یاد می‌گیرد.

انواع دیگر هوش مصنوعی:

سیستم‌های خبره رفتار یا قضاوت انسان را شبیه‌سازی می‌کنند. آنها دانش افراد متعدد را در حل مسئله ادغام می‌کنند و در تئوری راه‌حل‌های مؤثرتری ارائه می‌دهند. سیستم‌های خبره در تحقیقات شیمیایی برای تجزیه و تحلیل و پیش‌بینی ساختار مولکولی و در پزشکی برای تشخیص باکتری‌های مضر استفاده می‌شوند.

فناوری بینایی رایانه‌ای (Computer vision technology) در ترکیب با یادگیری عمیق(Deep Learning) ، ماشین‌ها را قادر می‌سازد تا تصاویر را تجزیه و تحلیل کنند. در حال حاضر در مراقبت‌های بهداشتی برای تشخیص و شناسایی ناهنجاری‌های بیمار بر اساس اشعه ایکس، MRI یا سی‌تی اسکن استفاده می‌شود. تشخیص چهره (Facial recognition) شکل دیگری از بینایی رایانه‌ای است که کاربردهای متعددی دارد، از جمله احراز هویت هنگام تلاش برای دسترسی به حساب بانکی یا محدود کردن دسترسی فیزیکی به ساختمان‌هایی که داده‌های حساس را در خود جای داده‌اند.

در حالی که رباتیک (Robotics) و هوش مصنوعی (AI) زمینه‌های متمایزی هستند، این دو اغلب با هم جفت می‌شوند تا ابزارهای نوظهوری ایجاد کنند که می‌توانند در دنیای واقعی مورد استفاده قرار گیرند. به عنوان مثال، ربات‌های فیزیکی که از حسگرهای بصری و پردازش تصویر استفاده می‌کنند، از هوش مصنوعی برای یادگیری نحوه پیمایش در محیط خود استفاده می‌کنند. تولید، کشاورزی و کالاهای بسته‌بندی شده مصرفی همگی صنایعی هستند که برای ایجاد کارآیی و افزایش بهره‌وری در عملیات خود، به رباتیک همراه با هوش مصنوعی حافظه محدود نیز متکی هستند. استفاده از جراحی‌های رباتیک و با کمک هوش مصنوعی در صنعت مراقبت‌های بهداشتی دقت بیشتری را ترویج می‌کند که می‌تواند منجر به بهبودی سریعتر بیمار شود.

نظریه ذهن هوش مصنوعی

در حالیکه امروزه نظریه ذهن هوش مصنوعی وجود ندارد، هدف از تحقیقات فعلی توسعه سیستم‌های هوش مصنوعی است که فاکتورهای ظریف مانند احساسات و انگیزه‌ها را به شیوه‌ای شبیه به انسان درک کرده و با آنها تعامل داشته باشند. کارهای در حال انجام در این زمینه شامل تلاش‌هایی برای توسعه سیستم‌هایی است که می‌توانند بر اساس ورودی‌های صدا، حالات چهره و احساسات، انسان‌ها را در زمان واقعی تجزیه و تحلیل کرده و با آنها تعامل داشته باشند و به شیوه‌ای شبیه به انسان پاسخ دهند.

هوش مصنوعی خودآگاه

هوش مصنوعی خودآگاه، مانند هوش مصنوعی نظریه ذهن، در حال حاضر نظری است و در عمل وجود ندارد. این نوع هوش مصنوعی که نزدیکترین ارتباط را با بحث‌های اخیر در مورد امکان "AGI" یا هوش مصنوعی عمومی (artificial general intelligence) دارد، نسخه فرضی از هوش مصنوعی است که به طور منحصر به فردی خودآگاه است و دارای آنچه بسیاری تصور می‌کنند یک آگاهی درونی غنی است که با توانایی‌های انسان مطابقت دارد یا از آن فراتر می‌رود. در حالی که این موضوع در ماه‌های اخیر یک نکته بحث‌برانگیز بوده است، بحث در مورد امکان‌پذیری این سطح از عملکرد هوش مصنوعی ادامه دارد.

بخش دوم

آغاز به کار

با تداوم استقرار هوش مصنوعی در سازمان‌ها به روش‌های مختلف، حسابرسان داخلی باید فعالانه عمل کرده و از نزدیک با مدیریت همکاری کنند تا استراتژی کلی سازمان خود را برای هوش مصنوعی، نحوه استفاده فعلی از هوش مصنوعی و برنامه‌ریزی‌های آتی برای استفاده از آن را درک کنند. به‌ویژه در طول فرآیند برنامه‌ریزی، حسابرسان داخلی باید با تحقیق و جمع‌آوری اطلاعات مرتبط در مورد استفاده بالقوه از هوش مصنوعی مورد بررسی از منابع داخلی و خارجی متعدد شروع کنند.

اطلاعات داخلی مهم می‌تواند شامل موارد زیر باشد:

- سیاست‌ها و رویه‌هایی که به هوش مصنوعی اشاره دارند، که می‌توان برای شناخت بهتر فرآیندهای سازمانی جمع‌آوری و بررسی کرد.
- طرح های استراتژیک مستند شده یک سازمان یا طرح استراتژیک، از جمله جنبه‌های هوش مصنوعی.
- گزارش‌های اخیر هیأت‌مدیره که حاوی دیدگاه و اطلاعات در مورد نحوه بحث رهبری و هیأت‌مدیره در مورد موضوعاتی مانند استفاده از هوش مصنوعی و نگرانی‌های مربوط به ریسک است.
- اطلاعات به دست آمده در طول جلسات ارزیابی ریسک مداوم با ذینفعان.

منابع خارجی می‌توانند چارچوب مرجع بیشتری را ارائه دهند، زیرا حسابرسان داخلی بررسی استراتژی هوش مصنوعی سازمان خود را آغاز می‌کنند. منابع خارجی ارزشمند ممکن است شامل موارد زیر باشد:

- سه بخش دیدگاه‌ها و بینش‌های جهانی : IIA انقلاب هوش مصنوعی.[۱۴]
- مجموعه ۱۰۱ هوش مصنوعی IIA .
- کنفرانس مجازی تجزیه و تحلیل، اتوماسیون و هوش مصنوعی IIA .
- منابع اصلی حسابرسی فناوری اطلاعات و امنیت سایبری مانند گواهینامه‌های IIA در حسابرسی برنامه امنیت سایبری و کنترل‌های عمومی فناوری اطلاعات. Practice Guides
- راهنماهای عمل IIA و راهنماهای حسابرسی فناوری جهانی (GTAG).
- چارچوب مدیریت ریسک هوش مصنوعی (AI RMF 1.0).
- دستورالعمل‌های مرکز ملی امنیت سایبری برای توسعه سیستم هوش مصنوعی ایمن.[۱۵]
- دستور اجرایی هوش مصنوعی کاخ سفید در اکتبر ۲۰۲۳.[۱۶]
- کتاب الکترونیکی راهبری هوش مصنوعی IBM .[۱۷]

محیط کنترل در سطح واحد تجاری : اجرا و استراتژی

هنگامی که حسابرسان خود را به این منابع مجهز کردند، پرسیدن این سوال که "هوش مصنوعی چگونه استفاده می شود؟" یک سوال ساده و مؤثر برای شروع جمع آوری اطلاعات است. پاسخ این سوال به احتمال زیاد مستلزم پرسش از افراد یا بخش‌های متعدد است، زیرا بسیاری از سازمان‌ها نه مدیریت متمرکزی بر هوش مصنوعی دارند و نه سیاست‌های مدون (از جمله تعریف هوش مصنوعی)، رویه‌ها یا استراتژی در مورد استفاده قابل قبول از هوش مصنوعی دارند.

برای سازمان‌هایی که هوش مصنوعی در آنها مستقر و توسعه یافته است، حسابرس داخلی باید با تیم هوش مصنوعی/علم داده گفتگو کند. این گفتگو باید شامل این باشد که از آنها بخواهید توضیح دهند که کدام هوش مصنوعی/الگوریتم‌ها مستقر شده‌اند، از جمله عملکرد، منابع داده‌های مورد استفاده، کاربرد، محدودیت‌ها، ریسک‌ها و پیامدهای اخلاقی آنها. حسابرسان داخلی همچنین باید از این موضوع شناخت کسب کنند که چه کنترل‌های موجودی برای کمک به مدیریت ریسک‌های ناشی از هوش مصنوعی وجود دارد - یا این که آیا مدیریت کنترل‌های جدیدی را در رابطه با استفاده و استقرار سیستم‌های هوش مصنوعی خود اجرا کرده است یا خیر. به دست آوردن شناخت اولیه از طراحی کنترل‌های مورد استفاده برای مدیریت ریسک‌های مربوط به هوش مصنوعی یک گام مهم است که می‌تواند همزمان با این بحث‌های اولیه انجام شود.

برای سازمان‌هایی که مشخص نیست که آیا هوش مصنوعی به طور رسمی یا غیررسمی مورد استفاده قرار می‌گیرد یا خیر واحد فناوری اطلاعات سازمان یک نقطه شروع خوب است، زیرا همانطور که در بخش سطوح پذیرش در قسمت ۱ ذکر شد، به نظر می‌رسد رهبران فناوری تمایل بیشتری به آزمایش و استفاده از هوش مصنوعی در بخش خود دارند. اگر فناوری اطلاعات تایید کند که هوش مصنوعی استفاده می‌شود، یا اگر بررسی‌های اولیه مشخص کند که هوش مصنوعی در سازمان استفاده می‌شود، پرسش منطقی بعدی تعیین میزان استفاده از هوش مصنوعی است.

در حالی که یک مصاحبه اولیه با تیم هوش مصنوعی/علم داده یا مدیریت فناوری اطلاعات یک گام اولیه خوب است، این بحث نباید محدود به این گروه‌ها باشد. از این بحث‌های اولیه، حسابرسان داخلی ممکن است دریابند که سایر بخش‌ها یا کاربران فردی از هوش مصنوعی برای عملکرد خاص خود استفاده می‌کنند که مستلزم مصاحبه‌های اضافی است. توصیه می‌شود با مدیریت برای بررسی یا همکاری در ایجاد فهرستی از بخش‌هایی که در حال حاضر از هوش مصنوعی استفاده می‌کنند و به روز رسانی مکرر آن فهرست، همکاری کنید.

این فهرست باید شامل سایر جنبه‌های کلیدی مانند هدف یا مقصود هوش مصنوعی، چه کسی از آن استفاده می کند، چه کسی آن را مدیریت می‌کند، ابزارهای خاص هوش مصنوعی مورد استفاده، ملاحظات مربوط به ریسک و چه کسی بر آن نظارت دارد، باشد. فرآیند بررسی یا همکاری با مدیریت برای توسعه یک فهرست هوش مصنوعی همچنین می‌تواند در طول فرآیند ارزیابی ریسک سالانه انجام شود.

اکثر حسابرسان داخلی از نزدیک با مدیر ارشد مالی (CFO) خود در رابطه با آزمون کنترل‌های داخلی بر گزارشگری مالی یا سایر مدیران اجرایی مانند مدیر ارشد امنیت اطلاعات (CISO)، مدیر ارشد اطلاعات (CIO) و غیره کار می‌کنند، بنابراین داشتن آن رابطه حرفه ای با تیم رهبری اجرایی (اعضای C-suite) باید فرصت دیگری برای گفتگوهای اولیه در مورد هوش مصنوعی فراهم کند. سؤالات مهمی که حسابرسان داخلی می‌توانند از مدیران خود بپرسند عبارتند از:

- آیا یک استراتژی هوش مصنوعی ایجاد شده است و اگر چنین است، جزئیات آن استراتژی چیست (از جمله جنبه‌هایی مانند استفاده از هوش مصنوعی برای به حداکثر رساندن کارآیی عملیات یا استفاده از هوش مصنوعی برای کاهش هزینه‌ها)؟"
- آیا تیم رهبری اجرایی (اعضای C-suite) تعیین کرده‌اند که چه کسی مسئول مدیریت ریسک‌های مربوط به هوش مصنوعی است؟"
- آیا تیم رهبری اجرایی (اعضای C-suite) چه نقشی در تعامل با هیأت‌مدیره (یا معادل آن) برای ملاحظات راهبری هوش مصنوعی ایفا می‌کند؟"

در این مرحله، حسابرسان داخلی موارد زیر را انجام داده‌اند:

- در رابطه با هوش مصنوعی در سازمان خود تحقیق و منابع خارجی را بررسی کرده‌اند.
- گفتگوهای اولیه هوش مصنوعی را با مدیریت، از جمله تیم هوش مصنوعی/علم داده یا مدیریت فناوری اطلاعات (یا هر دو) و تیم رهبری اجرایی (CFO، CISO، CIO و ...) انجام داده‌اند.
- با مدیریت در بررسی یا تدوین یک فهرست برای ثبت نحوه استفاده از هوش مصنوعی (یا برنامه‌ریزی برای استفاده در آینده) همکاری کرده‌اند.
- فرآیند شناخت این که چه راهبری برای هوش مصنوعی وجود دارد را آغاز کرده‌اند.

انجام این چهار کار نشان می دهد که حسابرسی داخلی اولین گام ها را در ایجاد یک دانش پایه از هوش مصنوعی در سازمان برداشته است. این کار همچنین فرصتی را برای حسابرسی داخلی فراهم می‌کند تا هرگونه مشاهدات فوری را که باید به موقع به مدیریت اطلاع داده شود، برجسته کند.

داده

پس از اینکه حسابرسان داخلی شناخت اساسی از نحوه استفاده از هوش مصنوعی پیدا کردند، باید دانش قوی‌تری در مورد استفاده از هوش مصنوعی در سازمان ایجاد کنند. از آنجایی که الگوریتم‌های مورد استفاده برای پشتیبانی از هوش مصنوعی به حجم زیادی از داده‌ها (که "کلان داده" نیز نامیده می‌شود) وابسته است، تعیین اینکه چه داده‌های سازمانی در یک برنامه کاربردی هوش مصنوعی معین استفاده می‌شود و نحوه مدیریت این داده‌ها بسیار مهم است. یک الگوریتم مجموعه‌ای از قوانین برای پیروی هوش مصنوعی است و همان چیزی است که یک ماشین را قادر می‌سازد تا به سرعت مقادیر عظیمی از داده‌ها را پردازش کند که یک انسان نمی‌تواند به طور منطقی با همان سهولت یا سرعت پردازش کند. با توجه به توانایی هوش مصنوعی در دریافت سریع و پاسخگویی به مقادیر زیادی از مجموعه‌های داده متنوع، معماری، عملکرد و دقت الگوریتم‌های درگیر بسیار مهم است.

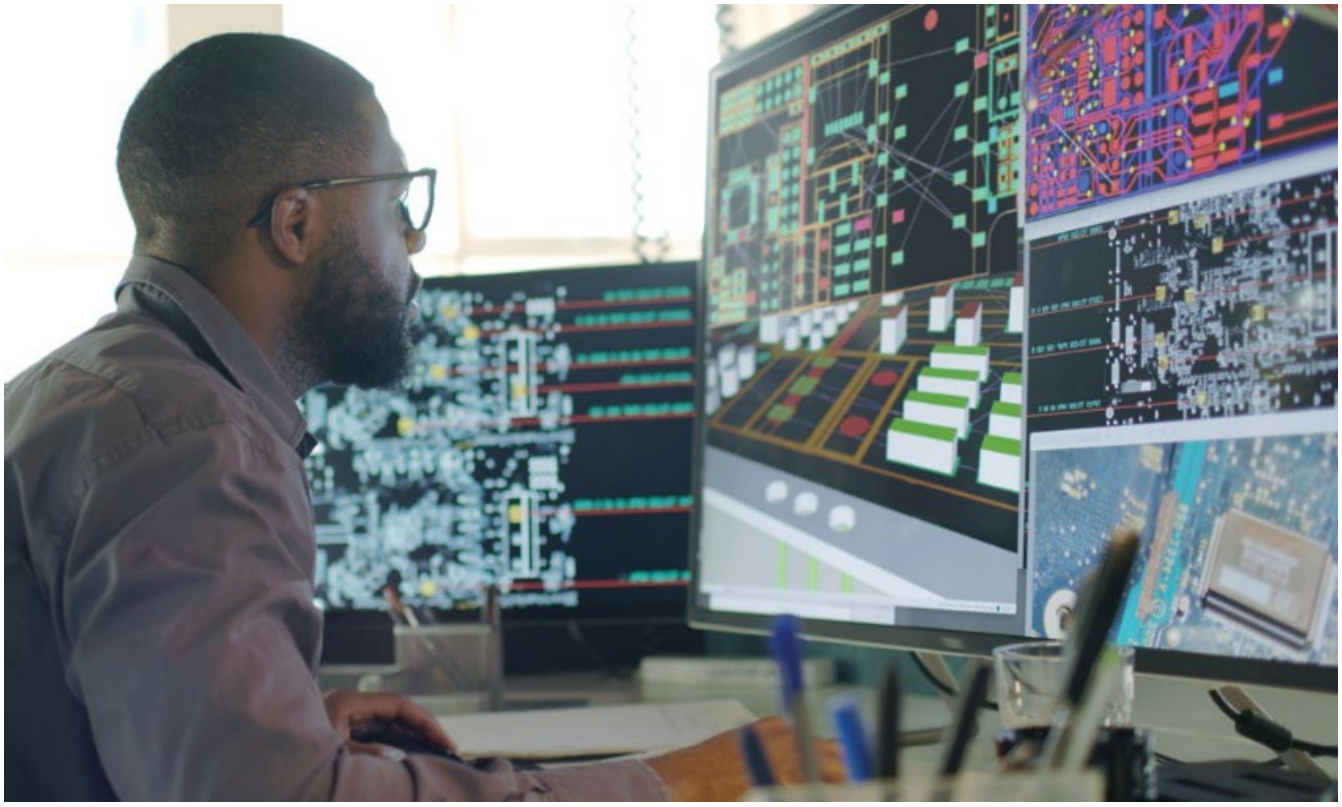
الگوریتم‌ها در ابتدا توسط انسان‌ها توسعه داده می‌شوند، بنابراین خطاهای انسانی و سوگیری‌ها (هم عمدی و هم غیرعمدی) می‌توانند بر عملکرد الگوریتم تأثیر بگذارند. بخش ۳ این چارچوب جزئیات بیشتری را در مورد ریسک‌های مربوط به خطاها و سوگیری‌های الگوریتم ارائه می‌دهد.

خارج از هوش مصنوعی، بسیاری از سازمان‌ها در حال حاضر استراتژی‌ای برای جمع‌آوری، ذخیره‌سازی، استفاده، مدیریت و حفاظت از داده‌ها تدوین کرده‌اند.

هوش مصنوعی مانند سایر برنامه‌های کاربردی داده‌محور است، به این معنا که همان جنبه‌های مهم در مورد داده‌ها مرتبط هستند و باید در نظر گرفته شوند، که شامل یکپارچگی، حریم خصوصی، محرمانه بودن، اعتبار، صحت و کامل بودن است.

کلان داده به معنای بیش از فقط مقادیر زیادی از داده است - کلان داده به داده‌هایی اشاره دارد که به حجم، تنوع، سرعت و تغییرپذیری بسیار بالایی می‌رسند که سازمان‌ها در معماری‌های سیستم، ابزارها و رویه‌هایی سرمایه‌گذاری می‌کنند که به طور خاص برای مدیریت داده‌ها طراحی شده‌اند. بسیاری از این داده‌ها ممکن است توسط خود سازمان تولید شوند، در حالی که سایر داده‌ها ممکن است در دسترس عموم باشند یا از منابع خارجی خریداری شوند. برای راهنمایی جامع در مورد شناخت و حسابرسی کلان داده، از جمله بحث در مورد فرصت‌ها و ریسک‌ها، و یک برنامه کاری نمونه، به "GTAG: شناخت و حسابرسی کلان داده" از IIA مراجعه کنید.

یکی دیگر از جنبه‌های مهم هم در استفاده از داده و هم در برنامه‌های کاربردی مرتبط با هوش مصنوعی، این است که آیا داده‌ها توسط طرفی خارج از سازمان میزبانی یا پردازش می‌شوند یا خیر. حسابرسان داخلی باید همیشه ریسک‌های مربوط به معاملات شخص ثالث (و چهارم) را در نظر بگیرند، زیرا محیط‌های کنترل داخلی فروشندگان ممکن است به اندازه محیط سازمان (یا چارچوب کنترلی محیط کنترل هوش مصنوعی فروشنده مورد نظر) جامع نباشد.



راهنمای عملی" IIA حسابرسی مدیریت ریسک شخص ثالث" رویکردی دقیق‌تر در مورد ریسک‌های مربوط به استفاده از فروشندگان خارجی در اختیار حسابرسان داخلی قرار می‌دهد.

یکی دیگر از جنبه‌های مهم داده، دسترسی کاربر است. شناخت اینکه چه کسی می‌تواند داده‌ها را ویرایش یا تغییر دهد، حیاتی است، زیرا دستکاری مجموعه داده‌ها از منظر ورودی، قطعاً می‌تواند بر خروجی پایین‌دستی هوش مصنوعی تأثیر بگذارد. شناخت و مستندسازی دسترسی کاربر مدیر به داده‌های متکی به هوش مصنوعی نیز ضروری است. " GTAG : حسابرسی هویت و مدیریت دسترسی IIA" نگاهی دقیق‌تر به ملاحظات حسابرسی داخلی مربوط به نحوه اطمینان سازمان از دسترسی مناسب کاربران به منابع فناوری اطلاعات ارائه می‌دهد.

امنیت سایبری

امنیت سایبری نیز باید مورد توجه قرار گیرد، زیرا مربوط به محدود کردن کاربران غیرمجاز از دسترسی به داده‌ها و اطمینان از حریم خصوصی، محرمانه بودن و محافظت از داده‌ها است. پذیرش و تکامل هوش مصنوعی، سازمان‌ها را مجبور می‌کند تا بر قابلیت‌های انعطاف‌پذیری سایبری خود تاکید مجدد کنند. از آنجایی که هوش مصنوعی قدرتمندتر می‌شود و تصمیمات بیشتری به الگوریتم‌های جدید، پیچیده و مبهم با استفاده از مجموعه‌های داده بزرگ سپرده می‌شود، محافظت از این سیستم‌ها در برابر نیروهای خارجی و مخرب برای موفقیت سازمانی حیاتی است. انعطاف‌پذیری سایبری برای هر سازمانی که از هوش مصنوعی استفاده می‌کند حیاتی است

حسابرسان داخلی معمولاً در آزمون اثربخشی کنترل‌های داخلی فناوری اطلاعات دخیل هستند. این آشنایی با نحوه پیاده‌سازی کنترل‌های داخلی مرتبط با امنیت سایبری توسط سازمان می‌تواند به حسابرسان داخلی در تأیید اینکه همان کنترل‌ها برای محافظت از داده‌های مرتبط با هوش مصنوعی استفاده می‌شوند، کمک کند.

نمونه‌هایی از کنترل‌های امنیت سایبری عبارتند از :

- استفاده از رمزگذاری.
- وجود نرم افزار آنتی ویروس.
- استفاده از سیستم های پیشگیری/تشخیص نفوذ.
- ثبت رویدادهای امنیتی هم درخواست ها و هم پاسخ‌ها.
- اطمینان از اینکه یک تست نفوذ به طور دوره‌ای برای جستجوی فعالانه آسیب پذیری ها انجام می شود
- آموزش کارکنان در بهترین شیوه‌ها برای شناسایی و جلوگیری از فیشینگ، سمیشینگ یا سایر طرح های مهندسی اجتماعی

برای جزئیات بیشتر، به" GTAG : حسابرسی عملیات امنیت سایبری: پیشگیری و تشخیص IIA " مراجعه کنید.

حسابرسان داخلی باید تعیین کنند که داده‌های متکی به هوش مصنوعی کجا ذخیره می‌شوند (داخلی، خارجی یا هر دو) و در نظر بگیرند که چه کنترل‌های امنیت سایبری در آنجا وجود دارد. برای داده‌های ذخیره شده به صورت خارجی، گزارش شرکت خدمات بازرسی سازمانی (SOC)باید برای آگاهی از محیط کنترلی فروشنده به دست آید. مدیریت باید از هرگونه نقص کنترلی که در گزارش شرکت خدمات بازرسی سازمانی (SOC)یافت می‌شود آگاه باشد و اطمینان حاصل کند که این نقص‌ها داده‌های متکی به هوش مصنوعی را در معرض خطر قرار نمی‌دهند. توافق نامه‌های سطح خدمات (SLA) با فروشندگان باید شامل یک بند "حق حسابرسی" باشد.

بخش ۳

چارچوب حسابرسی هوش مصنوعی

اولین نسخه چارچوب حسابرسی هوش مصنوعی IIA در سال ۲۰۱۷ منتشر شد. این چارچوب متخصصان حسابرسی داخلی را با رویکردی برای انجام خدمات مشاوره و اطمینان‌بخشی هوش مصنوعی به شیوه‌ای سیستماتیک و منظم ارائه می‌کرد. این نسخه به روزرسانی‌شده چارچوب، محتوا را با مثال‌هایی از محیط هوش مصنوعی فعلی مدرن‌سازی می‌کند، در حالی که جزئیات بیشتری را برای کمک به حسابرسان داخلی هم به‌عنوان مشاور و هم به عنوان ارائه دهنده اطمینان‌بخشی ارائه می‌دهد. این چارچوب دارای سه حوزه است.

چارچوب حسابرسی هوش مصنوعی

- ارکان راهبری
- مدیریت
- حسابرس داخلی

این چارچوب به مدل سه خط هوش مصنوعی IIA مرتبط است: ارکان راهبری بر مدیریت (خطوط اول و دوم) نظارت دارد، در حالی که نقش حسابرسی داخلی در حوزه سوم پوشش داده می‌شود، که شامل هر دو اطمینان‌بخشی مستقل (خط سوم) و فعالیت‌های مشاوره‌ای است.

چارچوب حسابرسی هوش مصنوعی IIA برای استفاده توسط حسابرسان داخلی در نظر گرفته شده است. با این حال، حوزه‌های راهبری و مدیریت چارچوب، فعالیت‌ها و عملکردهایی را خارج از حسابرسی داخلی که برای مدیریت هوش مصنوعی در یک سازمان مورد نیاز است، تشریح می‌کنند. هدف اصلی این چارچوب، تجهیز حسابرسان داخلی با دانش پایه اساسی هوش مصنوعی برای خدمت به سازمان خود به عنوان : ۱) مشاور مدیریت برای مشورت در مورد رویکرد کلی نحوه مدیریت، اجرا و نظارت بر هوش مصنوعی و/یا به عنوان ۲) ارائه دهنده اطمینان‌بخشی برای حسابرسی فرآیندها و کنترل‌هایی که مدیریت برای مدیریت، اجرا و نظارت بر هوش مصنوعی ایجاد کرده است

بلوغ سازمانی استفاده از هوش مصنوعی به نحوه استفاده از حسابرسی داخلی کمک می‌کند. به عنوان مثال، سازمان‌هایی که از نظر هوش مصنوعی کمتر بالغ هستند، ممکن است به حسابرسی داخلی نیاز داشته باشند تا در اکتشاف اولیه هوش مصنوعی نقش مشاور را ایفا کند، در حالی که یک سازمان بالغ‌تر در زمینه هوش مصنوعی احتمالاً حسابرسی داخلی را برای ارائه فعالیت‌های اطمینان‌بخشی، مانند ارزیابی فرآیندهای تثبیت‌شده و کنترل‌های داخلی برای اثربخشی عملیاتی، درگیر می‌کند. برای انجام موفقیت‌آمیز هر دو نقش، حسابرسی داخلی به شناخت درستی از نحوه مدیریت هوش مصنوعی و نحوه مدیریت فعلی آن توسط سازمان نیاز دارد.

ارکان راهبری - اولین حوزه این چارچوب - بر اساس رویکرد سازمان در برنامه‌ریزی استراتژیک هوش مصنوعی و ارائه نظارت و پایش نحوه برنامه‌ریزی، مدیریت و اجرای هوش مصنوعی توسط مدیریت است. ارکان راهبری به اطلاعاتی متکی است که توسط واحد حسابرسی داخلی در اختیار آنها قرار می‌گیرد.

ارتباط مشاوره‌ای با نهادهای راهبری مانند کمیته حسابرسی، هیأت‌مدیره یا نهاد راهبری معادل آن و این ارتباط باید شامل موضوعات نوظهوری مانند هوش مصنوعی باشد که چالش‌های نظارتی جدیدی را ارائه می‌کند.

حوزه **"مدیریت"** این چارچوب، رویکردی را تشریح می‌کند که سازمان هنگام برنامه‌ریزی و اجرای هوش مصنوعی در داخل سازمان از آن استفاده می‌کند. محیط کنترل داخلی پیرامون هوش مصنوعی توسط مدیریت در "خط اول" ایجاد می‌شود. همچنین شامل جنبه‌های استراتژیک مانند تعیین اهداف و مقاصد مرتبط با برنامه استراتژیک کلی هوش مصنوعی است. حسابرسی داخلی باید اطمینان حاصل کند که جهت استراتژیک هوش مصنوعی برای سازمان و رویکرد مدیریت برای مدیریت هوش مصنوعی را شناخته است.

حوزه "مدیریت" این چارچوب همچنین شامل جنبه‌های نظارتی "خط دوم" هوش مصنوعی است، مانند اینکه مدیریت ریسک سازمانی هنگام نظارت بر "خط اول" چه جنبه‌هایی را باید در نظر بگیرد. اغلب انتظار می‌رود حسابرسی داخلی در فرآیند ارزیابی ریسک یک سازمان شرکت کند. این حوزه برای حسابرسی داخلی مرتبط خواهد بود، زیرا دانش خود را از ریسک‌های مرتبط با هوش مصنوعی حفظ می‌کند.

حوزه سوم چارچوب، **"حسابرسی داخلی"**، شامل جنبه‌هایی از فعالیت‌های مشاوره‌ای برای مدیریت و ارائه خدمات اطمینان‌بخشی در ظرفیت حسابرسی ("خط سوم") است. حسابرسی داخلی می‌تواند از این چارچوب به عنوان نقطه شروع در هر دو نقش هنگام وظیفه‌یافتن برای شرکت در وظایف مرتبط با هوش مصنوعی استفاده کند.

از آنجا که هوش مصنوعی به سرعت در حال تکامل است، این چارچوب به به‌روزرسانی‌های دوره‌ای نیاز خواهد داشت. این تکامل، همراه با ماهیت پیچیده هوش مصنوعی، به این معنی است که حسابرسی داخلی احتمالاً فقط قادر به ارائه اطمینان محدود خواهد بود. این چارچوب به تنهایی ممکن است همه جنبه‌های هوش مصنوعی را پوشش ندهد، اما پایه محکمی را برای حسابرسان داخلی در هنگام توسعه دانش اساسی هوش مصنوعی به عنوان یک موضوع حسابرسی فراهم می‌کند.

راهبری

راهبری هوش مصنوعی به ساختارها، فرآیندها و رویه‌هایی اشاره دارد که برای هدایت، مدیریت و نظارت بر فعالیت‌های هوش مصنوعی سازمان پیاده‌سازی شده‌اند. راهبری شامل کمک به اطمینان از این است که فعالیت‌ها، تصمیمات و اقدامات هوش مصنوعی مطابق با ارزش‌های سازمان و همچنین مسئولیت‌های اخلاقی، اجتماعی و قانونی آن است. همچنین شامل ارائه نظارت برای اطمینان از اینکه آن دسته از کارمندانی که مسئولیت‌های هوش مصنوعی دارند، مهارت‌ها و تخصص لازم را دارند، می‌شود.

همانطور که در مدل سه خط منعکس شده است، حسابرسی داخلی به عنوان "خط سوم" عمل می‌کند و اطمینان مستقل و عینی از اعتبار سنجی کنترل‌های داخلی مورد استفاده سازمان برای مدیریت ریسک‌ها، از جمله تمام جنبه‌های هوش مصنوعی، ارائه می‌دهد. حسابرسی داخلی می‌تواند خدمات مشاوره‌ای مرتبط با هوش مصنوعی را به سازمان ارائه دهد، اما از دیدگاه راهبری، ارکان راهبری به شدت به فعالیت‌های اطمینان‌بخشی ارائه شده توسط حسابرسی داخلی برای شناخت بهتر اثربخشی عملیاتی سازمان متکی است.

راهبری هوش مصنوعی حیاتی است. دو مورد از مهمترین نقش‌هایی که راهبری ایفا می‌کند، ارزیابی این است که سازمان تا چه حد عملیات هوش مصنوعی را مدیریت می‌کند و اینکه آیا اهداف و مقاصد استراتژیک هوش مصنوعی سازمان به شیوه‌ای مطابق با ارزش‌های تعیین‌شده محقق می‌شوند یا خیر. همانطور که در بخش‌های قبلی ارائه شد، تعدادی ریسک خاص هوش مصنوعی وجود دارد. با این حال، یکی از ملاحظات اصلی، ارائه نظارت است که هوش مصنوعی به گونه‌ای مورد استفاده قرار گیرد که باعث آسیب نشود.

استراتژی

یک طرح استراتژیک به یک سازمان اجازه می‌دهد تا جهت و چشم‌انداز مورد نیاز برای دستیابی به اهداف خود را روشن و بیان کند. همین امر در مورد استراتژی هوش مصنوعی نیز صادق است. استراتژی هوش مصنوعی هر سازمان باید منحصر به فرد باشد و بر اساس رویکرد آن برای بهره‌گیری از فرصت‌هایی باشد که هوش مصنوعی فراهم می‌کند، در حالی که نسبت به شرایط خاص سازمان مانند جزئیات خدمات فناوری فعلی یا طرح های مستمر راهبری داده آگاه باشد. یک رویکرد استراتژیک هوش مصنوعی متفکرانه و روشمند از توانایی سازمان برای متمرکز کردن منابع خود و ارتقای همسویی در بین همه کارکنان ضمن کاهش ریسک‌های احتمالی پشتیبانی می‌کند.

دو نکته مهم را باید در نظر داشت:

۱.برنامه‌ریزی برای استراتژی هوش مصنوعی یک رویداد یکباره نیست. این یک فرآیند مکرر است که باید به طور دوره‌ای انجام شود. حسابرسی داخلی باید با مدیریت همکاری کند تا یک جدول زمانی برای بررسی استراتژی هوش مصنوعی تعیین کند.

۲.یک استراتژی هوش مصنوعی نباید به صورت مجزا برنامه‌ریزی شود. با توجه به دامنه منابع داده و موارد استفاده بالقوه، استراتژی‌های هوش مصنوعی سازمانی باید چندمنظوره باشند. با توجه به اهمیت حیاتی هوش مصنوعی، احتمالاً مشارکت و نظارت در سطح هیأت‌مدیره رخ خواهد داد، زیرا هوش مصنوعی این پتانسیل را دارد که به طور چشمگیری استراتژی‌های تجاری را تغییر دهد یا اصلاح کند

پرداختن به این نکات کمک خواهد کرد تا اطمینان حاصل شود که طرح های هوش مصنوعی از اهداف کلی سازمان پشتیبانی کرده و با ارزش‌های سازمانی اعلام شده همسو هستند. تدوین اهداف برای هوش مصنوعی به سازمان‌ها اجازه می‌دهد تا ملاحظات استراتژیک مهم را چارچوب‌بندی کنند، از جمله پاسخ به سؤالات اساسی مانند "چرا از هوش مصنوعی استفاده می‌کنیم؟" و "قصد داریم به چه چیزی دست یابیم؟" اهداف هوش مصنوعی باید مانند سایر اهداف سازمانی - مشخص، قابل اندازه‌گیری، دست‌یافتنی، مرتبط و مبتنی بر زمان - توسعه یابند تا از پذیرش ابزارها و خدمات هوش مصنوعی بدون دامنه مشخصی از دلیل سازمان برای انجام این کار، جلوگیری شود. [۱۸]

ویژگی‌های مطلوب هوش مصنوعی باید در هنگام تعیین اهداف، مقاصد و انتظارات گنجانده شوند. انتظارات یا اهداف سازمانی ممکن است شامل ویژگی‌های مطلوب زیر برای هوش مصنوعی باشد:

نگرش و رویکرد کلی سازمان نسبت به ریسک و مدیریت ریسک باید یک ملاحظه اولیه در هنگام توسعه یا به‌روزرسانی طرح استراتژیک و اهداف هوش مصنوعی باشد. داشتن یک ریسک‌پذیری بالاتر در راستای اهداف هوش مصنوعی ممکن است برای سازمانی که در جنبه‌های دیگر ریسک‌گریز است، مناسب نباشد، در حالی که سازمان‌هایی که از نظر تاریخی تحمل ریسک بالایی داشته‌اند، ممکن است تمایل بیشتری به پذیرش ریسک‌های مربوط به هوش مصنوعی داشته باشند. صرف‌نظر از میزان تحمل ریسک یک سازمان، تشخیص و نقشه‌برداری از ریسک‌های هوش مصنوعی در طول برنامه‌ریزی استراتژیک هوش مصنوعی ضروری است. [۱۹]

مدیریت - خط اول و دوم

در توسعه استراتژی هوش مصنوعی، مدیریت مسئول اطمینان از این است که کنترل‌های داخلی به درستی طراحی شده‌اند و به طور موثر برای کاهش ریسک عمل می‌کنند. همانطور که در بخش‌های قبلی توضیح داده شد، کنترل‌های داخلی موثر یک الزام حیاتی برای هوش مصنوعی هستند. بسیاری از سازمان‌ها نتایج کنترل‌های فناوری اطلاعات را به صورت فصلی و/یا سالانه آزمون و گزارش می‌کنند.

مدیریت باید از هرگونه مشکل کنترل داخلی که می‌تواند بر استفاده از هوش مصنوعی نیز تأثیر بگذارد، به ویژه در زمینه‌هایی از محیط کنترل داخلی که در حال حاضر ارزیابی می‌شوند، مانند موارد زیر آگاه باشد:

- یکپارچگی و راهبری داده.
- دسترسی کاربر.
- امنیت سایبری.
- چرخه حیات توسعه سیستم.
- مدیریت تغییر.
- کنترل‌های پشتیبان‌گیری/ بازیابی.

COBIT و COSO نمونه‌هایی از چارچوب‌های کنترل داخلی هستند که می‌توانند توسط سازمان‌ها برای کمک به رویکرد و ارزیابی محیط کنترل داخلی مورد استفاده قرار گیرند. [۲۰،۲۱]

مدیریت خط اول

راهبری

تعریف نقش‌ها و مسئولیت‌های مربوط به طرح‌های مبتنی بر هوش مصنوعی، سازمان را در تعیین منابع مورد نیاز برای فعالیت موثر پشتیبانی می‌کند. تشخیص مالک اجرایی، در حالی که ورود سایر اعضای تیم رهبری اجرایی (C-suite) را در نظر می‌گیرد، به اطمینان از پاسخگویی کمک می‌کند.

یک تیم رهبری هوش مصنوعی متشکل از اعضای بین‌بخشی، راه دیگری است که سازمان‌ها می‌توانند طرح‌های هوش مصنوعی را نظارت و اطلاع‌رسانی کرده و از پاسخگویی حمایت کنند. چنین تیمی باید شامل موارد زیر باشد:

- مدیران هوش مصنوعی و/یا علم داده.
- مدیر ارشد امنیت اطلاعات سازمان (CISO).

- پرسنل کلیدی فناوری اطلاعات.
- بخش حقوقی (برای ارائه راهنمایی در مورد ملاحظات نظارتی).
- بخش مالی/حسابداری برای پیگیری هزینه‌ها و بازگشت سرمایه پروژه‌های هوش مصنوعی.
- مدیریت ریسک.
- انطباق.

حسابرسی داخلی، با گستردگی دانش خود در مورد سازمان، در موقعیت منحصر به فردی قرار دارد تا به عنوان مشاور برای پشتیبانی از طرح‌های هوش مصنوعی خدمت کند و باید به عنوان عضوی از تیم رهبری هوش مصنوعی در نظر گرفته شود. مشارکت حسابرسی داخلی باید به گونه‌ای ساختاردهی شود که استقلال آن به عنوان یک ارائه دهنده اطمینان بخشی، به خطر نیفتد.

یک فرآیند برنامه‌ریزی اندیشمندانه، سازمان را در هنگام اجرای پروژه‌های هوش مصنوعی پشتیبانی خواهد کرد. کارمندانی که در اجرای پروژه‌ها دخیل هستند، باید از مهم‌ترین ریسک‌ها، از جمله نتایج ناخواسته، آگاه باشند. تأکید و اطمینان از اینکه اجرای روزانه پروژه‌ها شامل آگاهی در مورد جنبه‌های اجتماعی، اخلاقی، زیست‌محیطی و اقتصادی است، مهم است. علاوه بر این، ایجاد محیطی که کارمندان را تشویق به بحث آزادانه درباره ایده‌ها و نگرانی‌های مربوط به طرح های هوش مصنوعی می‌کند، می‌تواند به ایجاد فرهنگ شفافیت، آگاهی و مسئولیت متقابل برای حمایت از پروژه‌های جاه‌طلبانه هوش مصنوعی کمک کند.

خط‌مشی‌ها و رویه‌ها – استفاده داخلی و کاربردهای تجاری

تعریف، پذیرش و انتشار خط‌مشی‌ها و رویه‌های سازمانی قوی در مورد استفاده از هوش مصنوعی در داخل سازمان، جنبه مهم دیگری از استراتژی هوش مصنوعی یک سازمان است. خط‌مشی‌ها و رویه‌های صریح و روشن، به کارمندانی که مستقیماً در طرح‌های هوش مصنوعی دخیل هستند و به کارمندانی که ممکن است از هوش مصنوعی به عنوان بخشی از مسئولیت‌های کاری روزانه خود استفاده کنند، جهت می‌دهند. تدوین یک خط‌مشی استفاده قابل قبول از هوش مصنوعی باید اولویت اصلی سازمانی باشد. این خط‌مشی باید شامل جنبه‌هایی از بهترین شیوه‌های امنیت سایبری، ملاحظات مالکیت معنوی/حقوقی و ریسک‌های مرتبط با ابزارهای مختلف هوش مصنوعی باشد. این خط‌مشی باید با یک فرآیند مستند تکمیل شود که کاربران هنگام درخواست استفاده از هوش مصنوعی باید از آن پیروی کنند. استفاده از یک فرآیند تایید رسمی برای استفاده از هوش مصنوعی نیز از تلاش‌های سازمان برای حفظ فهرست کاربران یا بخش‌هایی که از هوش مصنوعی استفاده می‌کنند، پشتیبانی خواهد کرد.

خط مشی‌ها و رویه‌هایی که دستورالعمل‌ها و انتظارات مورد استفاده برای توسعه، استقرار و نظارت بر طرح‌های هوش مصنوعی را روشن می‌کنند، این فرآیند را رسمیت می‌بخشند. آنها یک مبنا برای تایید اینکه آیا پروژه‌ها به شیوه‌ای سازگار با خط مشی‌های مصوب، اخلاق و فرهنگ کلی ریسک سازمانی در حال انجام هستند، ارائه می‌دهند. حسابرسان داخلی با توجه به دانش و تجربه خود در ارائه اطمینان بر خط مشی‌ها و رویه‌های کلیدی، در موقعیت منحصر به فردی برای ارائه بازخورد فوری در این مورد قرار دارند. در بسیاری از موارد، به عنوان یک نقطه شروع، خط مشی‌ها و رویه‌های موجود ممکن است اقدامات نسبتاً مؤثری برای کاهش ریسک‌های ناشی از توسعه هوش مصنوعی ارائه دهند. به عنوان مثال، سیستم‌های هوش مصنوعی که در حال توسعه هستند، ممکن است مشمول چرخه عمر توسعه سیستم (SDLC) یا فرآیندهای کنترل مدیریت تغییر موجود باشند. با گذشت زمان، با تکامل و ارتقای موارد استفاده از هوش مصنوعی توسط سازمان‌ها، قطعاً باید کنترل‌های بالغ‌تر یا جدیدتری در نظر گرفته شود.

بر این اساس، خط‌مشی‌ها و رویه‌هایی که انتظارات و دستورالعمل‌ها را برای اشخاص ثالث درگیر در طرح های هوش مصنوعی روشن می‌کنند نیز مهم هستند. هماهنگی بین تیم‌هایی که هوش مصنوعی را مدیریت می‌کنند و گروه سازمان که روابط شخص ثالث را مدیریت می‌کند (مانند حقوقی) روابط سازگار با فروشندگان هوش مصنوعی را ترویج می‌کند. از آنجا که اشخاص ثالث، امتدادی از فرآیندهای سازمان هستند، شناخت خوب داشتن از محیط‌های کنترل فروشندگان بسیار مهم خواهد بود. در صورت وجود، مدیریت باید گزارش‌های شرکت خدمات بازرسی سازمانی (SOC) فروشندگان هوش مصنوعی را برای شناخت فرآیندهای کنترلی آنها و آگاهی از هرگونه نگرانی مانند یافته‌های حسابرسی، دریافت کند. استفاده از هر شخص ثالث مرتبط با توسعه قابلیت‌های هوش مصنوعی یا پشتیبانی مداوم از طرح های هوش مصنوعی باید به وضوح تعریف و نظارت شود، از جمله توافق‌نامه‌های سطح خدمات (SLA)که شامل حق حسابرسی است.

هنگامی که این خط‌مشی‌ها و رویه‌ها مشخص شدند، سازمان‌ها می‌توانند با به اشتراک گذاشتن اسناد خط‌مشی سازمانی پیش‌نویس شده مانند خط‌مشی استفاده قابل قبول در بین تمام کارکنان و دعوت از بازخورد در طول یک دوره اظهار نظر آزاد، خرید متقابل عملکردی خط‌مشی‌ها و رویه‌های هوش مصنوعی را ترویج دهند. سازمان‌ها همچنین باید برای منابع مورد نیاز برای آموزش کارکنان در مورد این خط‌مشی‌های جدید برنامه‌ریزی کنند تا اطمینان حاصل شود که کارکنان برای پذیرش و رعایت نقش‌ها، کنترل‌ها و مسئولیت‌های تازه تعریف شده مرتبط با استفاده از هوش مصنوعی آماده هستند. [۲۲]

منابع فناوری اطلاعات برای پشتیبانی از هوش مصنوعی

بهینه‌سازی مؤثر منابع فناوری اطلاعات برای پشتیبانی از طرح های هوش مصنوعی مورد نیاز است و باید بر این اساس توسط مدیریت بودجه‌بندی شود. استفاده از هوش مصنوعی نیازمند عملکرد فشرده دارایی‌های رایانه‌ای برای پایداری است.

پردازش قابل اعتماد. نمونه‌هایی از قابلیت‌های منابع فناوری اطلاعات IT مورد استفاده برای پشتیبانی از طرح های هوش مصنوعی یک سازمان عبارتند از:

- **واحدهای پردازش مرکزی (CPU)** – "مغز" کامپیوتر؛ پردازنده‌هایی که دستورات یا دستورالعمل‌ها را اجرا می‌کنند. [۲۳]
- **واحدهای پردازش گرافیکی (GPU)** - مغزهای تواناتر که می‌توانند قطعات زیادی از داده‌ها را به طور همزمان با قابلیت‌های ریاضی اضافی پردازش کنند؛ قادر به تولید گرافیک، تصاویر هستند و بیشتر در هوش مصنوعی تولید خلاق رایج هستند. [۲۴]
- **ذخیره سازی –** محل داده‌هایی که برای پردازش توسط هوش مصنوعی مورد نیاز است. ذخیره‌سازی معمولاً بر حسب ترابایت (۱۰۰۰ گیگابایت) یا پتابایت (۱۰۰۰ ترابایت) اندازه‌گیری می‌شود. به عنوان مثال، یک ویدیوی۵ تا ۱۰ دقیقه‌ای با کیفیت بالا تقریباً یک گیگابایت (۱ میلیارد بایت) اندازه دارد. سرورهای میزبانی شده در محل یا راه حل‌های مبتنی بر ابر نمونه‌هایی از مکان‌هایی هستند که داده‌ها ممکن است در آن ذخیره شوند.
- **حافظه** همچنین به عنوان رم RAM (حافظه دسترسی تصادفی) نامیده می‌شود. مکانی که داده‌های کوتاه مدت در آن ذخیره می شوند و سریعتر از داده‌های ذخیره‌سازی در دسترس هستند. بر حسب گیگابایت اندازه‌گیری می‌شود، جایی که ایستگاه های کاری رایانه‌ای منفرد دارای ۸ تا ۴۸ گیگابایت رم هستند. هرچه هوش مصنوعی در حال اجرا پیچیده‌تر باشد، رم بیشتری مورد نیاز است
- **ابررایانه ها –** سریعترین رایانه‌های پردازشی که برای محاسبات با کارآیی بالا استفاده می‌شوند و دارای CPU های متعددی هستند.
- **ایستگاه‌های کاری –** شامل رایانه‌های رومیزی و لپ تاپ با مشخصات فنی است که از الزامات هوش مصنوعی مورد استفاده پشتیبانی می‌کند.
- **نرم افزار** – پلتفرم‌ها، برنامه‌ها و برنامه‌هایی که برای توسعه، استقرار و مدیریت هوش مصنوعی استفاده می‌شوند. نرم‌افزار توسعه. نمونه‌ها عبارتند از IBM Watsonx.ai،Microsoft Azure AI و Platform Google Cloud AI. نرم افزار استقرار، که برای ادغام هوش مصنوعی در برنامه‌های موجود استفاده می‌شود. نمونه ها عبارتند از Docker و MLflow.
- **اتصال شبکه** این یک دسته‌بندی گسترده است که شامل سخت افزار، نرم‌افزار و خدماتی است که به کاربران اجازه می‌دهد منابع دیجیتال را به اشتراک بگذارند و اطلاعات را مبادله کنند. نمونه ها عبارتند از سرورهای فایل و روترها.

در حالی که از حسابرسان داخلی انتظار نمی‌رود که تمام مشخصات فنی و جزئیات الزامات هوش مصنوعی را بدانند، آنها باید دانش اولیه‌ای از منابع فناوری اطلاعاتIT داشته باشند

کارگزینی و آموزش

کارگزینی مناسب یک عنصر مهم در استراتژی هوش مصنوعی یک سازمان است. منابع انسانی باید با مدیریت همکاری کند تا اطمینان حاصل شود که کارمندانی با تجربه هوش مصنوعی مورد نیاز در سراسر سازمان استخدام می‌شوند. تجربه هوش مصنوعی باید نه تنها برای کارمندانی که وظیفه مدیریت جنبه‌های روزمره هوش مصنوعی را بر عهده دارند، بلکه برای رهبری که طرح های هوش مصنوعی را هدایت می‌کنند، در اولویت قرار گیرد.

از آنجا که هوش مصنوعی به سرعت در حال توسعه است، مهم است که کارکنان سازمان از پیشرفت‌ها و ریسک‌های مربوط آگاه باشند. سازمان ها باید اطمینان حاصل کنند که آموزش عمومی آگاهی از هوش مصنوعی به همه کارکنان ارائه می‌شود و فرصت‌های آموزشی فنی بیشتری مانند سمینارها، آموزش آنلاین یا دوره‌های آموزشی در اختیار کارمندانی که بر طرح های هوش مصنوعی تمرکز دارند، قرار می‌گیرد.

همانطور که در بالا در بخش سیاست‌ها و رویه‌ها ذکر شد، اجرای آموزش در مورد سیاست رسمی استفاده قابل قبول از هوش مصنوعی و گنجاندن هوش مصنوعی در دفترچه راهنمای کارمند و در توجیه کارمندان جدید راه‌های خوبی برای افزایش آگاهی سازمانی از هوش مصنوعی همراه با ریسک‌های احتمالی است. با ادغام طرح های آموزشی متمرکز بر هوش مصنوعی و سواد دیجیتال، سیاست‌ها و رویه‌های سازمانی و فرصت‌های ارتقای مهارت، سازمان‌ها می‌توانند از طریق سرمایه‌گذاری مستقیم در اعضای فعلی و جدید کارکنان از طرح های هوش مصنوعی پشتیبانی کنند. اجرا و نتایج این طرح‌ها باید توسط حسابرسی داخلی به عنوان بخشی از کنترل‌های هوش مصنوعی یک سازمان نظارت شود.

اجرا

مدیریت ریسک توسط خطوط اول و دوم

بخش ۲ در مورد اهمیت شناسایی ریسک‌های هوش مصنوعی مربوط به امنیت، یکپارچگی، حریم خصوصی و محرمانه بودن داده‌ها بحث کرد و رسیدگی به این نگرانی‌ها باید در حین اجرای پروژه‌های هوش مصنوعی توسط سازمان مورد توجه قرار گیرد. الگوریتم‌های هوش مصنوعی به داده‌های دقیق و قابل اعتماد متکی هستند و تیم‌های پروژه باید داده‌های ورودی را از نزدیک نظارت کنند. سازمان‌ها راه‌های متعددی برای اعتبارسنجی کامل بودن داده های مورد استفاده در پروژه‌های هوش مصنوعی دارند.

شامل حصول اطمینان از تطابق جمع کل رکوردها و تجزیه و تحلیل گزارش خطای هنگام انتقال داده بین سیستم‌ها. مدیریت باید کنترل‌های داخلی را طراحی و نظارت کند که ناهنجاری‌ها را در کیفیت یا کامل بودن داده‌ها تشخیص دهد.

سایر ملاحظات مهم داده شامل محدود کردن دسترسی کاربران فقط به کارمندانی است که روی یک پروژه هوش مصنوعی کار می‌کنند، که شامل دسترسی مدیر سیستم نیز می‌شود. تعیین نقش‌های کاربری و اطمینان از تفکیک وظایف مناسب نیز بسیار مهم است. به عنوان مثال، مدیران پایگاه داده بر داده‌های ورودی زیربنایی نظارت می‌کنند و نباید به تغییر الگوریتم‌هایی که آن داده‌ها را پردازش می‌کنند، دسترسی داشته باشند. وظیفه‌ای که به طور سنتی بر عهده یک توسعه‌دهنده است.

هنگامی که یک پروژه هوش مصنوعی در حال پیاده‌سازی است، مهم است که سازمان اطمینان حاصل کند که پروژه شفاف، قابل توضیح، مسئولانه و قابل حسابرسی است:

- ***شفافیت*** - قادر به شناخت آسان هدف هوش مصنوعی یا الگوریتم با اصطلاحات ساده
- ***قابلیت توضیح*** - قادر به توضیح مکانیسم‌ها، محاسبات یا نتایج پردازش شده توسط هوش مصنوعی یا الگوریتم
- ***مسئولیت پذیری*** - استفاده از هوش مصنوعی یا الگوریتم‌ها به شیوه‌ای اخلاقی، ایمن، منصفانه و قابل اعتماد

- ***قابلیت حسابرسی*** - از آنجایی که برنامه‌های هوش مصنوعی ممکن است شروع به جایگزینی یا تقویت برخی از فرآیندهای کلیدی انطباق یا سایر فرآیندهای مهم تجاری کنند، حفظ قابلیت ردیابی از طریق گزارش‌های حسابرسی موثر یا اطلاعات مرتبط، جزء مهمی برای توسعه هوش مصنوعی خواهد بود، زیرا اطمینان از این فرآیندها احتمالاً برای بسیاری از موارد استفاده بالقوه مورد نیاز خواهد بود.

مدیریت پروژه هوش مصنوعی باید جنبه‌های زیر را برای هر طرح تعریف کند:

- ***اهداف، نقش‌ها و زمان‌بندی*** – طرح اجرایی قصد دارد به چه چیزی دست یابد، چه کسی شرکت می‌کند و چه زمانی رخ می‌دهد
- ***الزامات منابع*** - برای دستیابی به موفقیت به چه فناوری و/یا منابع کارکنان نیاز است
- ***الزامات داده*** - چه داده‌های ورودی توسط هوش مصنوعی یا الگوریتم(ها) مورد نیاز است
- ***الزامات حریم خصوصی، قانونی و نظارتی*** - الزامات انطباق مرتبط چیست
- ***ارزیابی ریسک*** – ریسک‌های مربوط که دستیابی به اهداف پروژه یا نتایج ناخواسته را تهدید می‌کنند، مانند سوگیری‌ها، رفتار غیراخلاقی یا سوء استفاده چیست.

- ***معیارها یا شاخص‌های کلیدی عملکرد*** - (KPI) نحوه نظارت و کمی‌سازی موفقیت پروژه

- ***الزامات آزمون*** - در یک نقطه زمانی، نحوه اعتبارسنجی عملکرد هوش مصنوعی یا الگوریتم مطابق با طراحی و تغییرات مورد نیاز چیست. این شامل هر دو کاربر نهایی (که در نهایت از هوش مصنوعی استفاده می‌کنند) و متخصصان هوش مصنوعی/علم داده خواهد بود. تشخیص و اطلاع‌رسانی مسائل در این مرحله حیاتی خواهد بود. بررسی نحوه آزمون و تایید اثربخشی الگوریتم‌های توسعه‌دهندگان شخص ثالث، نکته مهمی است.

- ***الزامات آزمون*** - از دیدگاه تداوم، از آنجایی که خروجی هوش مصنوعی، به دلیل ماهیت خود، به دلیل ورودی داده تغییر می‌کند، باید به آزمون تداوم یا تضمین کیفیت در طول مدل توجه شود - بسته به مورد استفاده، این مفهوم ممکن است لازم باشد در الزامات تجاری یا طراحی هوش مصنوعی گنجانده شود.

نظارت مداوم بر پروژه‌های هوش مصنوعی باید توسط مدیریت انجام شود تا اطمینان حاصل شود که این طرح طبق برنامه پیش می‌رود و هرگونه مسئله یا نگرانی که رخ داده است شناسایی شود. همانطور که در مدل سه خط نشان داده شده است، مدیریت با ارائه اولین سطح اقدامات برای کاهش ریسک، نقش حیاتی در محیط کنترل داخلی ایفا می‌کند. نظارت در سطح پروژه مهم است زیرا مسائل در ابتدا در آنجا شناسایی می‌شوند. گزارش‌دهی مدیریت به هر دو رهبری اجرایی (C-suite) و هیأت‌مدیره باید بخشی از این فرآیند باشد. مهم است که نه تنها پیشرفت کلی پروژه را نظارت کنیم، بلکه هرگونه نتایج منفی، مانند هرگونه نگرانی اخلاقی یا نقض اطلاعات حساس را شناسایی و گزارش کنیم. گنجاندن ارزیابی از هر شخص ثالثی برای اطمینان از اینکه آنها مسئولیت‌های خود را در پروژه هوش مصنوعی انجام می‌دهند نیز مهم است.

نظارت و گزارش‌دهی همچنین باید شامل افشای هرگونه مسئله کنترل داخلی خاص پروژه یا تجزیه و تحلیل مسائل کنترل داخلی باشد که از سایر حوزه‌های سازمان ناشی شده و ممکن است بر پروژه هوش مصنوعی تأثیر بگذارد. مدیریت ریسک سازمانی و/یا تطبیق نیز باید از منظر "خط دوم" بخشی از فرآیند نظارت بر مسائل کنترل باشد.

پشتیبانی از خط دوم در مدیریت ریسک

اهداف اصلی فرآیند مدیریت ریسک سازمانی این است که درک کنیم چگونه ریسک‌ها ممکن است دستیابی به اهداف را تهدید کنند و سپس اقداماتی برای کاهش آن ریسک‌ها انجام دهیم.

دسته‌های ریسک شامل ریسک‌های استراتژیک، مالی، زیست محیطی، بازار، اجتماعی، اخلاقی، فناوری، اقتصادی، سیاسی، قانونی و نظارتی است. هوش مصنوعی موضوعی است که به طور کلی یک ریسک فناوری در نظر گرفته می‌شود. با این حال، مهم است که تشخیص دهیم ریسک هوش مصنوعی می‌تواند در هر یک از دسته‌های فوق قرار گیرد و نیاز به یک فرآیند مدیریت ریسک قوی برای پروژه‌های هوش مصنوعی دارد که هم نگرانی‌های فناوری و هم غیرفناوری را در نظر بگیرد.

چارچوب حسابرسی هوش مصنوعی IIA ملاحظات مدیریت ریسک را برای حمایت از پروژه‌های هوش مصنوعی سازمانی در پیروی از بهترین شیوه‌ها در مورد مدیریت ریسک هوش مصنوعی ارائه می‌دهد. در صورت لزوم، سایر چارچوب‌های موجود باید در نظر گرفته شوند، به ویژه چارچوب مدیریت ریسک هوش مصنوعیNIST . حسابرسان داخلی اغلب با متخصصان مدیریت ریسک در فعالیت‌هایی مانند فرآیند ارزیابی ریسک سالانه سازمان همکاری می‌کنند. بنابراین، بسیار مهم است که حسابرسان داخلی ریسک‌های مرتبط با هوش مصنوعی را درک کرده و به افزایش دانش خود ادامه دهند. علاوه بر این، حسابرسان داخلی باید ریسک‌های مرتبط با هوش مصنوعی را در سطح هر کار، یعنی هنگام حسابرسی فرآیندهایی که شامل جنبه‌ای از هوش مصنوعی هستند، در نظر بگیرند.

تشخیص

تشخیص ریسک‌های مرتبط با هوش مصنوعی ممکن است یک کار جدید برای بسیاری از سازمان‌ها باشد. در حالت ایده‌آل، مدیریت ریسک سازمانی (همراه با حسابرسی داخلی، تطبیق و حقوقی) در بحث‌های اولیه همه طرح‌های هوش مصنوعی برای کمک به چارچوب‌بندی ریسک‌های پیرامون پروژه هوش مصنوعی شرکت خواهد کرد. همانطور که در بخش استراتژی ذکر شد، یک تیم رهبری هوش مصنوعی بین‌بخشی یک راه موثر برای تشخیص فعالانه ریسک‌ها یا تهدیدهای بالقوه قبل از تحقق آنها است و در عین حال اطمینان حاصل می‌کند که کنترل‌ها و تکنیک‌های کاهش ریسک در سراسر سازمان وجود دارد.

سازمان‌هایی که قبلاً یک فرآیند ارزیابی ریسک در سطح سازمانی موثر ایجاد کرده‌اند، باید انجام یک ارزیابی ریسک اولیه متمرکز بر هوش مصنوعی را در نظر بگیرند. اگر یک ارزیابی ریسک جداگانه هوش مصنوعی امکان‌پذیر نیست، سازمان‌ها حداقل باید اطمینان حاصل کنند که هوش مصنوعی در طول فرآیند کلی ارزیابی ریسک گنجانده شده است.

به عنوان مثال، سازمان‌ها به طور دوره‌ای با تیم رهبری اجرایی درگیر می‌شوند تا ریسک‌ها را در حوزه‌های مختلف مشخص کنند. در بسیاری از موارد، بحث‌ها یا نظرسنجی‌ها شامل سوالات خاصی است، مانند "بزرگترین ریسک‌های استراتژیک سازمان چیست؟"

برای آوردن هوش مصنوعی به خط مقدم فرآیند ارزیابی ریسک، سازمان‌ها باید هوش مصنوعی را به عنوان یک حوزه ریسک نوظهور برجسته کنند، بازخورد مداوم از تیم رهبری هوش مصنوعی و/یا کارکنان داخلی را به اشتراک بگذارند و بر این اساس از مدیران اجرایی ورودی جمع‌آوری کنند. مرحله تشخیص ریسک در فرآیند مدیریت ریسک مهم است زیرا ممکن است ریسک‌هایی را برجسته کند که قبلاً مشخص نشده بودند.

سازمان‌هایی که یک استراتژی واضح هوش مصنوعی با اهداف و مقاصد مشخص ایجاد کرده‌اند، بستری را فراهم می‌کنند که مدیریت ریسک سازمانی برای کمک به تشخیص ریسک هوش مصنوعی به آن نیاز دارد. این بستر به مدیریت ریسک سازمانی اجازه می‌دهد تا فهرستی از ریسک‌هایی تهیه کند که دستیابی به آن اهداف و مقاصد را تهدید می‌کند و به سازمان‌ها اجازه می‌دهد تا در برنامه‌های استراتژیک خود محافظت‌هایی را در برابر آسیب‌های احتمالی ناشی از استفاده از هوش مصنوعی بگنجانند. برای سازمان‌ها مهم است که به این نکته توجه داشته باشند که چشم‌انداز ریسک پیرامون هوش مصنوعی به سرعت در حال تکامل است و پیامدهای منفی ناخواسته‌ای را از ریسک‌های حساب‌نشده ایجاد می‌کند که ممکن است شامل موارد زیر باشد: [۲۵]

- نتایج مغرضانه یا تبعیض‌آمیز که ممکن است به طور ناعادلانه بر بخش‌های خاصی از جامعه تأثیر بگذارد.
- به خطر افتادن حریم خصوصی یا محرمانه بودن.
- عدم پاسخگویی.
- نبود شفافیت.
- نبود قابلیت تبیین.
- آسیب مالی یا نابرابری اقتصادی.
- آسیب‌زیست محیطی.
- اطلاعات نادرست یا دستکاری.
- نقض حق تکثیر.

"جعبه سیاه"

در حالی که بسیاری از فرآیندهای تشخیص، ارزیابی و کاهش ریسک برای پروژه‌های هوش مصنوعی از بهترین شیوه‌های موجود پیروی می‌کنند، مهم است که توجه داشته باشیم "جعبه سیاه" هوش مصنوعی یک ریسک مجزا را ایجاد می‌کند. این اصطلاح به عدم شفافیت در سیستم‌های هوش مصنوعی و نحوه تصمیم‌گیری آنها اشاره دارد. شناخت مدل‌های یادگیری عمیق به ویژه با توجه به پردازش پیچیده انجام شده توسط الگوریتم‌ها همراه با دید یا شناخت بالقوه محدود یا بدون دید از نحوه تولید یک خروجی، می‌تواند دشوار باشد.

این می‌تواند چالش‌های خاصی را ایجاد کند زیرا مدیریت ریسک سازمانی (و حسابرسان داخلی) تلاش می‌کنند مستندات مورد نیاز برای پشتیبانی از چرخه مدیریت ریسک تعریف شده در بالا را ضبط کنند. متخصصان ریسک و حسابرسان داخلی می‌توانند مستقیماً "جعبه سیاه" را با این موارد برطرف کنند:

شناسایی و به وضوح اطلاع رسانی در مورد جایی که ممکن است اطلاعات مفقود یا ناقص در یک پروژه هوش مصنوعی داشته باشند.

- ***مثال***: اگر یک سازمان از یک فروشنده هوش مصنوعی شخص ثالث استفاده می‌کند که اطلاعات دقیقی در مورد داده‌های آموزشی یک الگوریتم ارائه نمی‌دهد، این باید مستند و به عنوان یک ریسک بالقوه افشا شود.

به طور مداوم ارزیابی و به روز رسانی هیأت‌مدیره در مورد اثرات بالقوه مربوط به شکاف‌های اطلاعاتی که شناسایی شده است.

- ***مثال***: هنگامی که عدم وجود مستندات فروشنده در مورد مجموعه آموزشی مستند شد، حسابرسان داخلی باید هیأت‌مدیره را در مواجهه با پیامدهای مرتبط با ریسک (مانند نمونه‌های متعدد از خروجی مغرضانه هوش مصنوعی که نشان دهنده مشکلاتی در داده‌های آموزشی است) به روز کنند.

ارائه راهنمایی در مورد چگونگی کاهش ریسک‌های مرتبط با شکاف‌های دانش "جعبه سیاه" که قبلاً مستند و ارزیابی شده‌اند.

- ***مثال***: بر اساس ارزیابی و پیامدهای ارائه شده، سازمان تصمیم می‌گیرد به یک فروشنده جدید هوش مصنوعی با مستندات داده شفاف‌تر مهاجرت کند.

ارزیابی

ارزیابی و تجزیه و تحلیل ریسک‌های شناسایی شده مرتبط با هوش مصنوعی باید از یک فرآیند مشابه استفاده کند که یک سازمان برای بررسی سایر ریسک‌ها استفاده می‌کند - ابتدا باید تأثیر و احتمال در نظر گرفته شود. کمیت‌سنجی تأثیر ریسک‌های مرتبط با هوش مصنوعی ممکن است به دلیل ملاحظات متعدد مانند پیامدهای قانونی، نظارتی، اجتماعی، مالی، زیست‌محیطی و اخلاقی دشوار باشد. آسیب به اعتبار برند یکی دیگر از ملاحظات برای تأثیر است.

ترکیب اثرگذاری و احتمال، منجر به ریسک ذاتی می‌شود که معیاری از ریسکی است که بدون در نظر گرفتن کنترل‌های داخلی وجود دارد. پس از ارزیابی ریسک ذاتی، ریسک باقیمانده باید تعیین شود، که شامل در نظر گرفتن این موضوع است که ریسک‌ها تا چه اندازه به خوبی کاهش یافته‌اند.

به عنوان نمونه‌ای از ارزیابی امنیت هوش مصنوعی به عنوان یک هدف، تهدیدات سایبری ممکن است به عنوان یک ریسک قابل توجه شناسایی شوند. برای مقابله با ریسک‌های سایبری، سازمان‌ها کنترل‌های امنیت سایبری را با هدف کاهش ریسک ذاتی به سطح قابل قبولی از ریسک باقیمانده، مستقر می‌کنند. اگر مدیریت ریسک سازمانی ارزیابی کند که ریسک باقیمانده به سطح قابل قبولی کاهش نیافته است، سازمان باید تصمیم بگیرد که چگونه ادامه دهد.

اولویت‌بندی ریسک فرآیندی است که یک سازمان برای رتبه‌بندی ریسک‌ها بر اساس اهمیت استفاده می‌کند، یعنی مهم‌ترین ریسک‌ها ابتدا مورد بررسی قرار می‌گیرند. سازمان‌ها منابع محدودی دارند اما با ریسک‌های نامحدودی روبرو هستند، بنابراین اطمینان از اینکه ریسک‌های مربوط به هوش مصنوعی در تجزیه و تحلیل گسترده‌تر ریسک در سطح کل سازمان اولویت‌بندی می‌شوند، مهم است. رتبه ریسک‌های مربوط به هوش مصنوعی در سازمان‌های مختلف بر اساس فرآیند ارزیابی ریسک، میزان استفاده آنها از هوش مصنوعی و سطح بلوغ محیط کنترل داخلی آنها متفاوت خواهد بود. به بیان ساده، هیچ رویکرد "یک اندازه برای همه" برای ارزیابی ریسک‌های مربوط به هوش مصنوعی وجود ندارد.

کاهش

کاهش ریسک یک اقدام (یا اقداماتی) است که مدیریت برای کاهش ریسک به سطح قابل قبول‌تر انجام می‌دهد. در بسیاری از موارد، سازمان‌ها ترجیح می‌دهند ریسک‌های مربوط به هوش مصنوعی را از طریق اقدامات کاهشی مانند افزودن کنترل‌های داخلی، مدیریت کنند. با این حال، پاسخ‌های احتمالی دیگری نیز برای ریسک وجود دارد، همانطور که در جدول زیر توضیح داده شده است. [۲۶]

عوامل متعددی بر نحوه تصمیم گیری سازمان در مورد نحوه پاسخ به ریسک‌های مربوط به هوش مصنوعی تأثیر می‌گذارند. بنابراین، داشتن یک فرآیند پاسخ به ریسک تعریف شده و تکرارپذیر بسیار حیاتی است. ریسک‌های مربوط به هوش مصنوعی ممکن است در طول یک پروژه تغییر کنند، بنابراین یک سازمان باید به طور مداوم نحوه پاسخ و کاهش ریسک‌ها را بررسی کند.

حسابرسی داخلی – فعالیت‌های مشاوره‌ای و اطمینان‌بخشی

پس از شرح نحوه رویکرد یک سازمان به هوش مصنوعی در دو دامنه چارچوب قبلی، یک دامنه باقی مانده وجود دارد - حسابرسی داخلی.

دو دامنه اول یک مبنا برای نحوه ارائه خدمات مشاوره‌ای و حسابرسی توسط حسابرسی داخلی به شرکت ارائه می‌دهند.

برخوردهای اساسی به ریسک

برخورد	ویژگی‌ها	تعریف
مدیریت کردن	کاهش، تخفیف، افزایش، بهره‌برداری، اهرم، بهینه سازی	اعمال کنترل برای کاهش ریسک ذاتی به یک سطح باقیمانده قابل قبول یا اعمال سایر اقدامات برای به حداکثر رساندن و استفاده از واریانس های احتمالی در نتایج.
تحمل کردن	پذیرفتن، دنبال کردن	تعیین اینکه آیا مزایای بالقوه، ریسک را توجیه می‌کند، با ایجاد اقدامات لازم برای کاهش یا اهرم احتمال و/یا تأثیر
انتقال دادن ▪	به اشتراک گذاشتن، پخش کردن	گسترش ریسک یا با انتقال تمام یا بخشی از آن به شخص ثالث (مانند بیمه یا برون سپاری)، یا استفاده از منابع چندین تیم برای جلوگیری از تلفات احتمالی.
خاتمه دادن	اجتناب کردن	خاتمه دادن یا اجتناب از ریسک با کنار گذاشتن اقدام برنامه ریزی شده یا حذف کامل هدف، اولویت بندی سایر اهداف در اولویت.

حوزه‌های راهبری و مدیریت حاوی جزئیاتی هستند که یک حسابرس داخلی باید از آنها برای مشاوره دادن به سازمان در مورد حرکت به سمت آن رویه‌ها یا ایجاد مبنایی برای ارزیابی نحوه رویکرد، استفاده، مدیریت و نظارت سازمان بر هوش مصنوعی استفاده کند.

"اطمینان معقول" اصطلاحی است که اغلب در حرفه حسابرسی داخلی به آن اشاره می‌شود. از منظر کنترل داخلی، اطمینان معقول به این معنی است که احتمال زیادی وجود دارد که کنترل‌ها ریسک را کاهش دهند، اما مطلق نیست. همین منطق باید برای حسابرسان داخلی که وظیفه ارائه اطمینان در مورد هوش مصنوعی را دارند، در نظر گرفته شود.

چالش‌ها

چندین جنبه از هوش مصنوعی، فعالیت های اطمینان بخشی را برای حسابرسان داخلی دشوار می‌کند، از جمله:

- هوش مصنوعی (یا به طور خاص تر، الگوریتم ها) ذاتاً بسیار پیچیده است - یک مسئله "جعبه سیاه" دشوارتر.
- قابلیت‌ها و ریسک‌های هوش مصنوعی با سرعت بالایی در حال افزایش هستند.
- هوش مصنوعی به عنوان یک موضوع حسابرسی با ابزارها یا رویکردهای پذیرفته شده گسترده، در حال تحول است.
- فرصت های آموزشی محدودی برای افزایش مجموعه مهارت‌های حسابرسی هوش مصنوعی در دسترس است.

هوش مصنوعی به عنوان یک موضوع حسابرسی می تواند طاقت فرسا به نظر برسد، اما تمرکز بر ملاحظات زیر به حسابرسان داخلی کمک می‌کند تا یک ذهنیت مثبت و مطمئن ایجاد کنند:

- از حسابرسان داخلی انتظار نمی‌رود که در مورد هر موضوع حسابرسی متخصص باشند. بلکه، داشتن یک رویکرد منظم و روشمند با تمرکز بر تفکر انتقادی و تشخیص ریسک باید هدف برای همه حسابرسی‌ها باشد، نه فقط هوش مصنوعی. آشنایی و دانش کاری از هوش مصنوعی حیاتی است. با این حال، دانستن تمام جنبه‌های فنی هوش مصنوعی محتمل نیست. ممکن است لازم باشد از منابع فنی خارجی برای کمک به جنبه‌های فنی‌تر مانند رمزگشایی الگوریتم‌ها استفاده شود.

- از آنجایی که هوش مصنوعی بسیار پیچیده و در حال تغییر است، بعید است که حسابرسان داخلی هرگز تسلط کاملی بر دانش این موضوع داشته باشند. حسابرسی هوش مصنوعی را به عنوان یک پیشرفت در نظر بگیرید، نه یک مقصد - شناخت خود را از هوش مصنوعی در طول زمان افزایش دهید.

- تمایل به پرسیدن سوالات مرتبط در مورد هوش مصنوعی در سازمان داشته باشید:

  - هوش مصنوعی چگونه به ما در دستیابی به اهداف استراتژیک کمک می‌کند؟
  - چه ریسک‌های وجود دارد و چگونه آنها را کاهش می‌دهیم؟
  - آیا کنترل‌های داخلی کافی در مورد فرآیندهای مرتبط با هوش مصنوعی وجود دارد؟
  - آیا داده‌هایی که برای هوش مصنوعی استفاده می‌شوند کامل، دقیق و قابل اعتماد هستند؟
  - هوش مصنوعی قبل از استقرار چگونه آزمایش می‌شود تا اطمینان حاصل شود که هیچ‌گونه سوگیری وجود ندارد؟
  - هوش مصنوعی پس از استقرار چگونه آزمایش می‌شود تا اطمینان حاصل شود که هیچ‌گونه سوگیری وجود ندارد؟
  - هوش مصنوعی چگونه اداره می‌شود؟
  - سازمان چگونه از آموزش و آگاهی کافی در مورد هوش مصنوعی اطمینان حاصل می‌کند؟

همانطور که در قسمت ۲ توضیح داده شد، شناخت استفاده سازمانی از هوش مصنوعی با تحقیق و بحث آغاز می‌شود. ضروری است که حسابرسان داخلی از روابط حرفه‌ای که ایجاد کرده‌اند استفاده کنند.

شفاف بودن با مدیریت و نهاد راهبری مهم است. به زبان ساده توضیح دهید که چگونه به هوش مصنوعی به عنوان یک موضوع فکر می‌کنید و چگونه قصد دارید سازمان را برای کسب اطلاعات بیشتر در مورد آن درگیر کنید.

حسابرسی‌های داخلی هوش مصنوعی یک مسئولیت نسبتاً جدید برای بسیاری از سازمان‌ها است. در حالی که به عنوان ارائه دهندگان اطمینان، انتظار نمی‌رود حسابرسان داخلی در مورد موضوع هوش مصنوعی متخصص باشند، اما باید فرصت‌هایی را برای افزایش دانش و آگاهی خود در مورد این موضوع مشخص کنند. شناخت بهتر جنبه‌های فنی‌تر هوش مصنوعی، مانند الگوریتم‌ها، برای آموزش حرفه‌ای آینده مهم خواهد بود.

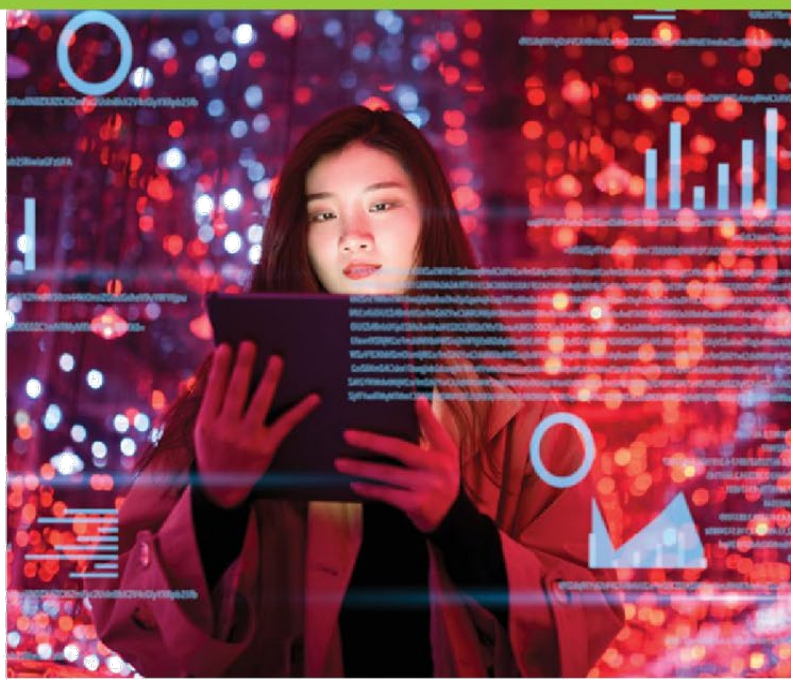
در حالی که هوش مصنوعی مطمئناً عناصر پیچیده ای دارد، مهم است به یاد داشته باشید که نوعی خروجی از ورودی‌هایی که دریافت می‌کند، تولید می‌کند. از منظر اطمینان، حسابرسان داخلی ممکن است هرگز دانش کاملی از تمام عملکردهای داخلی هوش مصنوعی نداشته باشند. با این حال، کمک به یک سازمان برای ۱) ارزیابی اینکه چه کاری انجام می دهند تا اطمینان حاصل شود که داده‌های ورودی تا حد امکان دقیق هستند، سپس ۲) شناخت اینکه چگونه آن خروجی مورد بررسی دقیق قرار می‌گیرد، باید اهداف اصلی متخصصان باشد. حسابرسان داخلی این مفاهیم را امروزه هنگام انجام حسابرسی‌های فناوری اطلاعات از طریق برنامه‌های کاربردی تجاری به کار می‌برند. وجه مشترک، مفهوم ردیابی است - اطمینان از اینکه داده‌ها و خروجی با اهداف کسب و کار و الزامات مورد استفاده هوش مصنوعی همسو هستند.

پاورقی

۱.. Britannica, “Artificial Intelligence..”
۲.. The IIA’s Three Lines Model..
۳.. A..M.. Turing, “Computing Machinery..”
۳.. A..L.. Samuel, “Checkers..”
۵.. McCarthy, Dartmouth..
۶.. Weizenbaum, “ELIZA..”
۷.. Humanoid Robot, “Waseda University..”
۸.. Hsu, “Raj Reddy..
۹.. “Prometheus Project..”
۱۰. . Britannica, “Deep Blue..”
۱۱. .IBM AI Adoption Index..
۱۲. . IBM “Different types of AI..”
۱۳. . Certes, “Types of AI..”
۱۴.. IIA Global Perspectives & Insights..
۱۵.. National Cybersecurity Centre..
۱۶.. White House Fact Sheet..
۱۷.. IBM AI Governance e-book..
۱۸. . Doran, “Smart Way..”
. . Moyer, ISACA, “Quantitative Approach..”
۲۰.. COBIT, “Framework..”
۲۱. . COSO, “Guidance..”
۲۲.. Deloitte, “3 Lines..”
۲۳.. “Gartner Glossary.”
۲۴.. Intel, “GPU.”
۲۵.. Forbes, 15 Biggest Risks..
۲۶.. IIA, CRMA..

بخش چهارم

راهنما و واژگان تخصصی



راهنمای فعالان یک چک‌لیست ساده است که حسابرسان داخلی می‌توانند از آن برای شروع ارزیابی خود از نحوه رویکرد، استفاده، مدیریت و گزارش سازمان در مورد هوش مصنوعی استفاده کنند. حسابرسان داخلی می‌توانند از نکات کلیدی ذکر شده در بخش‌های راهبری، مدیریت و حسابرسی داخلی قسمت ۳ برای توسعه برنامه حسابرسی خود یا به عنوان ملاحظات در نقش مشاوره استفاده کنند. بسیاری از جنبه‌ها یا ملاحظات در بخش اطمینان بخشی زیر ارتباط نزدیکی با مواردی دارند که قبلاً در سایر حوزه‌ها فهرست شده‌اند.

این چک‌لیست برای ارائه راهنمای شروع سریع است، اما باید بر اساس ملاحظات سازمانی، مانند میزان استفاده از هوش مصنوعی و اینکه آیا برنامه ریزی استراتژیک، خط‌مشی‌ها، رویه‌ها، فرآیندها و گزارش رسمی هوش مصنوعی ایجاد شده است، سفارشی شود.

مشخصات و ملاحظات	وضعیت / نتایج
ایجاد چشم‌انداز، استراتژی و اولویت‌بندی برای هوش مصنوعی و به‌روزرسانی مکرر آن.	
پیوند دادن ابتکار هوش مصنوعی به اهداف استراتژیک سازمان. (این ممکن است شامل موارد استفاده افزایش‌دهنده درآمد یا برنامه‌های کاربردی داخلی برای کاهش هزینه یا بهبود کارایی باشد.)	
اطمینان از اینکه جنبه‌های اخلاقی، سوگیری، اجتماعی و قانونی در استراتژی گنجانده شده‌اند.	
تعیین نحوه اندازه‌گیری موفقیت ابتکارات هوش مصنوعی، از جمله اهداف و بازگشت سرمایه **(ذ دد)** .	
اطمینان از اینکه طرح استراتژیک هوش مصنوعی با فرهنگ ریسک سازمان سازگار است.	
اطمینان از اینکه طرح استراتژیک هوش مصنوعی با ارزش‌های سازمان سازگار است.	
اطمینان از اینکه طرح استراتژیک هوش مصنوعی به طور رسمی به هیأت‌مدیره ابلاغ می‌شود.	
اطمینان از اینکه طرح استراتژیک شامل بهینه‌سازی منابع هوش مصنوعی است.	

مشخصات و ملاحظات	وضعیت / نتایج
اطمینان حاصل شود که محیط کنترل داخلی برای پشتیبانی از هوش مصنوعی مساعد است. در نظر بگیرید که چه تغییرات فوری در سیاست‌ها برای پشتیبانی از رشد هوش مصنوعی مورد نیاز است - برای مثال، افزودن سوالی در مورد استفاده از هوش مصنوعی در خط‌مشی مدیریت فروشندگان شخص ثالث.	
تعیین مدیریت اجرایی مسئول نظارت بر طرح‌های هوش مصنوعی.	
ایجاد یک تیم رهبری هوش مصنوعی بین‌بخشی برای نظارت بر همه طرح‌های هوش مصنوعی.	
اطمینان حاصل شود که تیم‌های حقوقی و تطبیق ، تمام الزامات نظارتی فعلی و نوظهور را رصد می‌کنند.	
تعیین نقش حسابرسی داخلی به عنوان مشاور و/یا ارائه دهنده خدمت اطمینان بخشی.	
اطمینان حاصل شود که مدل سه خط در جای خود قرار دارد و شامل هوش مصنوعی می‌شود.	
اطمینان حاصل شود که **حذف با**(یا معادل آن) در تمام طرح‌های هوش مصنوعی مشارکت دارد.	
اطمینان حاصل شود که نقش‌های شخص ثالث در طرح‌های هوش مصنوعی به وضوح تعریف و نظارت می شوند.	
اطمینان حاصل شود که امور مالی/حسابداری، بازگشت سرمایه را در طرح‌های هوش مصنوعی پیگیری می‌کند.	
تدوین خط‌مشی استفاده قابل قبول از هوش مصنوعی که برای همه کارکنان الزامی است.	
تدوین سیاست‌ها و رویه‌ها برای اجرا و حفظ طرح‌های هوش مصنوعی.	
تدوین سیاست‌ها و رویه‌ها برای طرح‌های هوش مصنوعی که از اشخاص ثالث استفاده می کنند.	
اطمینان حاصل شود که منابع فناوری اطلاعات برای پشتیبانی از طرح‌ها و کنترل‌های هوش مصنوعی کافی است.	
اطمینان حاصل شود که سطوح پرسنلی برای پشتیبانی از طرح‌ها و کنترل‌های هوش مصنوعی کافی است.	
اطمینان حاصل شود که استخدام منابع انسانی بر روی شیوه‌های استخدام متخصصان با تجربه در هوش مصنوعی تمرکز دارد.	
رهبری هوش مصنوعی دانش مدیریتی هوش مصنوعی مورد نیاز را حفظ می‌کند.	
کارکنان عملیاتی هوش مصنوعی دانش فنی مورد نیاز هوش مصنوعی را حفظ می‌کنند.	
همه کارکنان آموزش های لازم در مورد استفاده قابل قبول و ریسک‌های هوش مصنوعی را تکمیل می کنند.	
گنجاندن موضوع هوش مصنوعی در کتابچه راهنمای کارکنان و در توجیه پرسنل جدید.	
اطمینان حاصل شود که جنبه‌های منصفانه اجتماعی، زیست محیطی و اقتصادی در تمام پروژه‌های مرتبط با هوش مصنوعی در نظر گرفته می‌شود.	
اطمینان حاصل شود که داده‌های مرتبط با هوش مصنوعی ایمن، خصوصی و محرمانه هستند	
اطمینان حاصل شود که داده‌های مرتبط با هوش مصنوعی شفاف، قابل توضیح و مسئولانه هستند.	
تعریف اهداف، مقاصد، زمان‌بندی و الزامات منابع برای پروژه‌های هوش مصنوعی.	
تعریف مسئولیت‌های عملیاتی برای همه کارکنان ذیربط در پروژه‌های هوش مصنوعی.	
اطمینان حاصل شود که دسترسی کاربران به هوش مصنوعی متناسب با وظایف شغلی است.	
تعریف الزامات داده و ملاحظات مربوط به حریم خصوصی برای پروژه‌های هوش مصنوعی.	

ی در حال حاضر

مشخصات و ملاحظات	وضعیت / نتایج
تعریف الزامات قانونی و نظارتی قابل اعمال برای پروژه‌های هوش مصنوعی.	
انجام ارزیابی ریسک پروژه هوش مصنوعی برای شناسایی تهدیدات احتمالی برای موفقیت.	
تعریف سوگیری‌های احتمالی، از جمله ملاحظات اخلاقی و اجتماعی برای پروژه‌های هوش مصنوعی.	
تعریف معیارهای موفقیت یا شاخص‌های کلیدی عملکرد پروژه برای پروژه‌های هوش مصنوعی.	
ایجاد پارامترهای گزارش‌دهی مانند فرکانس، محتوا و نقاط عطف برای پروژه‌های هوش مصنوعی.	
ایجاد رویکرد آزمایشی برای تأیید اینکه هوش مصنوعی قبل و بعد از راه‌اندازی مطابق با هدف کار می‌کند.	
گزارش در مورد دستیابی به معیارها/شاخص‌های کلیدی عملکرد به رهبری اجرایی و هیأت‌مدیره.	
اطمینان حاصل شود که گزارش‌دهی شامل افشای سوگیری، نگرانی‌های اخلاقی یا اجتماعی است.	
اطمینان حاصل شود که گزارش‌دهی شامل انطباق با الزامات قانونی و نظارتی است.	
اطمینان حاصل شود که گزارش‌دهی شامل افشای هرگونه نتایج ناخواسته یا منفی است.	
اطمینان حاصل شود که گزارش‌دهی شامل افشای احتمالی از دست دادن داده‌ها یا نقض حریم خصوصی است.	
اطمینان حاصل شود که کنترل‌های داخلی مرتبط به طور دوره‌ای ارزیابی و گزارش می‌شوند.	
هوش مصنوعی را به عنوان بخشی از فرآیند مدیریت ریسک سازمانی (**چد پ)** قرار دهید.	
شناسایی خطراتی که اهداف و مقاصد استراتژیک هوش مصنوعی را تهدید می‌کنند.	
شناسایی خطراتی که ممکن است پیامدهای اخلاقی، اجتماعی، زیست‌محیطی یا مالی داشته باشند.	
شناسایی خطراتی که مربوط به استفاده از اشخاص ثالث برای هوش مصنوعی هستند.	
اطمینان حاصل شود که فرآیندی برای ثبت خطرات جدید یا نوظهور وجود دارد.	
اطمینان حاصل شود که کارکنانی که مسئولیت‌های مدیریت ریسک هوش مصنوعی را بر عهده دارند به درستی آموزش دیده‌اند.	
انجام ارزیابی ریسک مبتنی بر هوش مصنوعی و به روز رسانی دوره‌ای آن.	
الویت‌بندی خطرات مرتبط با هوش مصنوعی بر اساس امتیاز شدت (تأثیر و احتمال).	
اطمینان حاصل شود که فرآیندی برای انتخاب پاسخ‌های ریسک مناسب، از جمله نظارت بر پیشرفت پاسخ‌ها، وجود دارد.	
اطمینان حاصل شود که سازمان در مورد استراتژی، اهداف و مقاصد هوش مصنوعی با هیأت‌مدیره در تعامل است.	
اطمینان حاصل شود که سازمان به طور دوره‌ای به روز رسانی‌هایی را در مورد هوش مصنوعی به هیأت‌مدیره ارائه می‌دهد به نحوی که واضح و به راحتی قابل درک باشد.	
اطمینان حاصل شود که سازمان در مورد رویکرد مدیریت ریسک برای هوش مصنوعی با هیأت‌مدیره تعامل دارد.	
انجام تحقیقات داخلی و خارجی اولیه در مورد هوش مصنوعی.	
تعیین اینکه آیا استراتژی رسمی هوش مصنوعی تدوین شده است یا خیر.	

مشخصات و ملاحظات	وضعیت / نتایج
انجام بحث‌های اولیه با تیم هوش مصنوعی/علم داده (در صورت وجود) و/یا مدیریت فناوری اطلاعات.	
ایجاد فهرستی از کاربردهای فعلی و برنامه‌ریزی شده هوش مصنوعی.	
تدوین نحوه استفاده، اهداف و مقاصد برای استفاده فعلی هوش مصنوعی.	
تدوین شناخت رویکرد، نحوه ارزیابی ریسک‌ها و برنامه‌ریزی آزمایشی قبل از استقرار برای استفاده برنامه‌ریزی شده هوش مصنوعی.	
تدوین شناخت جنبه‌های زیر از داده‌های ورودی مرتبط با هوش مصنوعی: • راهبری. • معماری. • دسترسی کاربر. • کنترل های امنیت سایبری. • کنترل‌های پردازش (یکپارچگی، دقت، کامل بودن). • ملاحظات شخص ثالث (گزارش‌های SOC).	
تأیید کنید که چگونه هوش مصنوعی آزمایش و بررسی می‌شود تا اطمینان حاصل شود که به اهداف خود می‌رسد و عاری از سوگیری است، هم قبل و هم بعد از استقرار.	
تأیید کنید که طرح های هوش مصنوعی اهداف و مقاصد مشخصی دارند و پروژه‌ها توسط سطح مناسبی از رهبری مدیریت می‌شوند.	
تأیید کنید که گزارش‌دهی دوره ای به هیأت‌مدیره توسط مدیریت انجام می‌شود. تأیید کنید که هوش مصنوعی به عنوان بخشی از فرآیند مدیریت ریسک سازمانی در نظر گرفته می‌شود و شامل ریسک‌های مربوط به موارد زیر است: • اخلاق. • ملاحظات اجتماعی و اقتصادی. • جنبه‌های زیست محیطی. • پیامدهای مالی. • تخلفات قانونی و مقرراتی.	
تأیید کنید که سیاست‌ها و رویه‌هایی ایجاد شده است که نحوه استفاده و مدیریت هوش مصنوعی توسط سازمان را مشخص می‌کند، از جمله یک سیاست استفاده قابل قبول هوش مصنوعی.	
ایجاد شناخت از نحوه حمایت سازمان از یادگیری و آموزش هوش مصنوعی برای افزایش دانش و آگاهی برای تمام کارکنان.	

استانداردهای مرتبط با هوش مصنوعی

۶.۱ ماموریت حسابرسی داخلی.

۶.۲ منشور حسابرسی داخلی.

۶.۳ حمایت هیات‌مدیره و مدیریت ارشد.

۷.۱ استقلال سازمانی.

۷.۲ صلاحیت مدیر ارشد اجرایی حسابرسی.

۸.۱ تعامل هیات‌مدیره.

۸.۲ منابع.

۸.۳ کیفیت.

۸.۴ ارزیابی کیفیت خارجی.

واژه‌نامه

تعاریف اصطلاحاتی که با علامت ستاره مشخص شده‌اند، از واژه نامه چارچوب بین‌المللی اجرای حرفه‌ای ®IIA، نسخه ۲۰۱۷ گرفته شده است. سایر تعاریف یا برای اهداف این سند تعریف شده اند یا از منابع زیر گرفته شده‌اند:

IBM. “Explainers.” *IBM*. https://www.ibm.com/topics.

موسسه مدیریت ریسک. “فرهنگ ریسک”. موسسه مدیریت ریسک، ۲۰۲۳

https://www.theirm./what-we-say/thought-leadership/risk-culture/

اندرسون، اورتون; مایکل جی. هد; استیو مار; سریدهار رامامورتی; کریس ریدل; مارک سالماسیک; پل جی. سوبل. حسابرسی داخلی: خدمات اطمینان بخشی و مشاوره ای، ویرایش پنجم (Lake Mary, FL: ۲۰۲۲ .(بنیاد حسابرسی داخلی، https://www.theiia.org/products/bookstore/internal-auditing-assurance-andadvisory-services-5th-edition/

“واژه نامه ISACA ”،

ISACA. 2022. https://www.isaca resources/glossary

.”واژه نامه NIST“ . مرکز منابع امنیت رایانه

Gaithersburg, MD.: NIST. https://csrc.nist.gov/glos کارگروه مشترک . NIST SP 800-53، کنترل‌های امنیتی و حریم خصوصی برای سیستم‌ها و سازمان‌های اطلاعاتی، ویرایش ۵، پیوست الف: واژه نامه Gaithersburg, MD: . NIST، سپتامبر ۲۰۲۰ https://doi.org/10.6028/NIST.SP .

گراسی، پل; مایکل‌ای. گارسیا; جیمز ال. فنتون NI . SP 800-63-3، دستورالعمل‌های هویت دیجیتال، پیوست الف: تعاریف و اختصارات,Gaithersburg . MD: NIST، ژوئن ۲۰۱۷ https://doi.org/10.6028/NIST.SP.800 .

حسابرسی داخلی Sawyer، تقویت و محافظت، ارزش سازمانی، ویرایش هفتم (Lake Mary, FL) ، بنیاد حسابرسی داخلی، ۲۰۱۹ https://www.thei .

org/en/products/bookstore/sawyers-internal-auditingenhancing-and-protecting-organizational-value-7thedition/ Techopedia.com. “فرهنگ لغت فناوری”. https:// techopedia.com/dictiona

الگوریتم - یک فرآیند ریاضی صریح و مشخص برای محاسبه. مجموعه‌ای از قوانینی که در صورت پیروی از آنها، نتیجه‌ای معین به دست خواهد آمد. واژه نامه (NIST).

هوش مصنوعی - یک سیستم رایانه‌ای پیشرفته که می‌تواند قابلیت‌های انسانی مانند تجزیه و تحلیل را بر اساس مجموعه‌ای از قوانین از پیش تعیین شده، شبیه‌سازی کند. (ISACA) .

ارزیابی - فرآیند شناسایی ریسک‌ها برای عملیات سازمانی (شامل مأموریت، وظایف، تصویر، شهرت)، دارایی‌های سازمانی، افراد، سایر سازمان‌ها و کشور، ناشی از عملکرد یک سیستم اطلاعاتی. بخشی از ریسک مدیریت شامل تجزیه و تحلیل تهدید و آسیب‌پذیری می‌شود و تعدیل‌های ارائه شده توسط کنترل‌های امنیتی برنامه‌ریزی شده یا در محل را در نظر می‌گیرد. مترادف با تجزیه و تحلیل ریسک (واژه نامه NIST).

کمیته حسابرسی – کمیته‌ای از هیأت‌مدیره که مسئولیت پیشنهاد تأیید حسابرسان و گزارش‌های مالی به هیأت‌مدیره را دارند. (Sawyer’s).

پشتیبان‌گیری و بازیابی – فایل‌ها، تجهیزات، داده‌ها و رویه‌ها در صورت خرابی یا از دست دادن، برای استفاده در دسترس هستند، اگر نسخه‌های اصلی از بین رفته یا از سرویس خارج شده باشند (ISACA) .

پشتیبان‌گیری و بازیابی - به فرآیند پشتیبان‌گیری از داده‌ها در صورت از دست رفتن و راه‌اندازی سیستم‌ها اشاره دارد که امکان بازیابی داده‌ها را به دلیل از دست دادن آنها را فراهم می‌کند

پشتیبان‌گیری داده نیازمند کپی و بایگانی داده‌های کامپیوتری است، به‌طوری که در صورت حذف یا خراب شدن داده‌ها، قابل دسترسی باشد. داده‌های مربوط به زمان‌های گذشته فقط در صورت پشتیبان‌گیری قابل بازیابی هستند . (Techopedia)

کلان داده - اصطلاحی که برای اشاره به حجم زیاد اطلاعات دیجیتالی که به طور مداوم در حال جریان است، افزایش عظیم در ظرفیت ذخیره مقادیر زیادی از داده‌ها و میزان قدرت پردازش داده مورد نیاز برای مدیریت، تفسیر و تجزیه و تحلیل حجم‌های بزرگ اطلاعات دیجیتالی استفاده می‌شود. (حسابرسی داخلی، ویرایش پنجم)

تست جعبه سیاه - رویکردی برای آزمایش که بر عملکرد برنامه یا محصول متمرکز است و نیازی به دانش فواصل کد (code intervals) ندارد (ISACA) .

هیأت Board * - بالاترین سطح ارکان راهبری (به عنوان مثال، هیأت‌مدیره، هیأت‌نظارت یا هیأت‌امنا یا متولیان) که مسئولیت هدایت و/یا نظارت بر فعالیت‌های سازمان و پاسخگویی مدیریت ارشد را بر عهده دارد. اگرچه ترتیبات راهبری در حوزه‌های قضایی و بخش‌ها متفاوت است، اما معمولاً هیأت‌مدیره شامل اعضای مدیران اجرایی نیستند. اگر هیأت‌مدیره‌ای وجود نداشته باشد، کلمه "هیأت‌مدیره" در استانداردها به گروه یا شخصی اطلاق می‌شود که مسئولیت راهبری سازمان را بر عهده دارد. علاوه بر این، "هیأت‌مدیره" به کمیته یا رکنی دیگری اشاره دارد که ارکان راهبری وظایف خاصی را به آن تفویض کرده است (به عنوان مثال، کمیته حسابرسی).

چت‌بات - چت‌بات یک برنامه هوش مصنوعی است که با استفاده از عبارات کلیدی از پیش محاسبه شده کاربر و سیگنال‌های شنیداری یا متنی، مکالمه تعاملی انسان را شبیه‌سازی می‌کند. چت‌بات‌ها اغلب توسط سازمان‌ها برای ارائه خدمات مدیریت ارتباط با مشتری (CRM) به صورت ۲۴ ساعته استفاده می‌شوند. این نوع ربات نرم‌افزاری همچنین می‌تواند به عنوان یک دستیار مجازی هوشمند مورد استفاده قرار گیرد(Technopedia) .

علوم کامپیوتر - علوم کامپیوتر مطالعه سخت‌افزار و طراحی نرم افزار کامپیوتر است. همچنین شامل مطالعه الگوریتم‌های نظری و مشکلات عملی مربوط به پیاده‌سازی آنها از طریق سخت افزار و نرم افزار کامپیوتر است. مطالعه علوم کامپیوتر دارای شاخه‌های زیادی است، از جمله هوش مصنوعی، مهندسی نرم افزار، برنامه‌نویسی و گرافیک کامپیوتری(Technopedia).

امنیت سایبری - امنیت سایبری به هر فناوری، اقدام یا رویه‌ای برای جلوگیری از حملات سایبری یا کاهش تأثیر آنها اشاره دارد.

هدف امنیت سایبری محافظت از سیستم‌ها، برنامه‌ها، دستگاه‌های محاسباتی، داده‌های حساس و دارایی‌های مالی افراد و سازمان‌ها در برابر ویروس‌های رایانه‌ای ساده و آزاردهنده، حملات باج‌افزاری پیچیده و پرهزینه و هر چیزی بین این دو است (IBM) .

راهبری داده - راهبری داده به فرآیند مدیریت کیفیت داده‌ها در یک سازمان به منظور اطمینان از اینکه در تمام مراحل چرخه عمر خود، داده‌ها دقیق، در دسترس، سازگار، ایمن و قابل استفاده هستند، اشاره دارد. تحلیلگران کسب و کار و دانشمندان داده برای به دست آوردن بینش و شناخت از آن اطلاعات، در سراسر شرکت به دنبال اطلاعات هستند و از نیازهای تجاری پشتیبانی می‌کنند (IBM) .

درستی داده - خاصیتی که داده‌ها به طور غیرمجاز تغییر نکرده‌اند. یکپارچگی داده شامل پوشش‌دهی داده‌ها در هنگام ذخیره سازی، در حین پردازش و در حین انتقال است. (واژه نامه NIST).

یادگیری عمیق - یادگیری عمیق یک رویکرد تکراری برای هوش مصنوعی (AI) است که الگوریتم‌های یادگیری ماشین را در یک سلسله مراتب از افزایش پیچیدگی و انتزاع انباشته می‌کند. هر سطح یادگیری عمیق با دانش به دست آمده از لایه قبلی سلسله مراتب ایجاد می‌شود (Technopedia) .

تشخیص چهره - تشخیص چهره نوعی فناوری بیومتریک است که از داده‌ها برای تأیید وجود چهره یک انسان در یک تصویر دیجیتالی استفاده می‌کند. دو کاربرد اصلی برای نرم‌افزار تشخیص چهره وجود دارد: تشخیص و احراز هویت (Technopedia).

راهبری* - ترکیبی از فرآیندها و ساختارهایی که توسط هیأت‌مدیره اجرا می‌شود تا فعالیت‌های سازمان را در جهت دستیابی به اهداف خود مطلع، هدایت، مدیریت و نظارت کند.

کنترل داخلی - مکانیزم جامعی که یک سازمان برای دستیابی و نظارت بر اهداف سازمانی از آن استفاده می‌کند. (واژه نامه NIST).

مدل زبانی بزرگ - یک مدل زبانی بزرگ (LLM) نوعی مدل یادگیری ماشین است که می‌تواند انواع وظایف پردازش زبان طبیعی (NLP) را انجام دهد، مانند تولید و طبقه‌بندی متن، پاسخ دادن به سؤالات به روش محاوره‌ای و ترجمه متن از یک زبان به زبان دیگر. برچسب "بزرگ" به تعداد مقادیری (پارامترها) اشاره دارد که مدل زبانی می‌تواند به طور خودکار در حین یادگیری تغییر دهد. موفق‌ترین مدل‌های زبانی بزرگ (LLM) دارای صدها میلیارد پارامتر هستند. (تکنوپدیا)

یادگیری ماشین یادگیری ماشین (ML) زیرشاخه‌ای از هوش مصنوعی (AI) است که مدل‌های الگوریتمی را برای شناسایی الگوها و روابط در داده‌ها می‌سازد. در این زمینه، کلمه "ماشین" مترادف با برنامه کامپیوتری است و کلمه "یادگیری" شرح می‌دهد که چگونه الگوریتم‌های ML با دریافت داده‌های اضافی، دقیق‌تر می‌شوند. (تکنوپدیا)

موسسه ملی استاندارد و فناوری (NIST)

چارچوب مدیریت ریسک هوش مصنوعی(AI RMF) **موسسه ملی استاندارد و فناوری** (NIST) – همانطور که قانون ملی طرح هوش مصنوعی سال ۲۰۲۰ .P.L. (۲۸۳-۱۱۶بیان می‌کند، هدف چارچوب مدیریت ریسک هوش مصنوعی (AI RMF)، ارائه منبعی به سازمان‌هایی است که سیستم‌های هوش مصنوعی را طراحی، توسعه، استقرار یا استفاده می‌کنند تا به مدیریت ریسک‌های متعدد هوش مصنوعی کمک کرده و توسعه و استفاده قابل اعتماد و مسئولانه از سیستم‌های هوش مصنوعی را ترویج دهند. این چارچوب به گونه‌ای طراحی شده است که داوطلبانه، حافظ حقوق (rights-preserving) ، غیر اختصاصی (عمومی) و بی‌طرف باشد و انعطاف‌پذیری را برای سازمان‌ها در هر اندازه و در همه بخش‌ها و در سراسر جامعه فراهم کند تا رویکردهای موجود در چارچوب را پیاده‌سازی کنند. این چارچوب برای تجهیز سازمان‌ها و افراد - که در اینجا به عنوان کنشگران هوش مصنوعی از آنها یاد می‌شود - با رویکردهایی طراحی شده است که قابلیت اطمینان سیستم‌های هوش مصنوعی را افزایش داده و به پرورش طراحی، توسعه، استقرار و استفاده مسئولانه از سیستم‌های هوش مصنوعی در طول زمان کمک می‌کند.

ریسک چیزی که دستیابی به یک هدف را تهدید می‌کند.

تحمل ریسک* سطح ریسکی که یک سازمان مایل به پذیرش آن است.

فرهنگ ریسک فرهنگ ریسک اصطلاحی است که ارزش‌ها، باورها، دانش، نگرش‌ها و شناخت در مورد ریسک را که توسط گروهی از افراد با یک هدف مشترک به اشتراک گذاشته می‌شود، توصیف می‌کند. این امر در مورد همه سازمان‌ها - از جمله شرکت‌های خصوصی، نهادهای دولتی، دولت‌ها و سازمان‌های غیرانتفاعی - صدق می‌کند. (موسسه مدیریت ریسک)

رباتیک رباتیک مهندسی و بهره‌برداری از ماشین‌هایی است که می‌توانند به طور مستقل یا نیمه‌مستقل وظایف فیزیکی را از طرف انسان انجام دهند. به طور معمول، ربات‌ها وظایفی را انجام می‌دهند که یا بسیار تکراری هستند یا برای انسان بسیار خطرناک هستند که نمی‌توان آن را به طور ایمن انجام داد. (تکنوپدیا)

گزارش شرکت خدمات بازرسی سازمانی – (SOC) گزارش حسابرسی، تکمیل شده توسط ارزیاب مستقل، که محیط کنترل داخلی یک سازمان را ارزیابی می‌کند. می‌تواند توسط ارایه کنندگان خدمات به مشتریان ارائه شود تا اطمینان حاصل کنند که کنترل‌های داخلی آنها به طور موثر عمل می‌کنند.

تشخیص گفتار تشخیص گفتار، همچنین به عنوان تشخیص خودکار گفتار (ASR)، تشخیص گفتار کامپیوتری یا گفتار به متن شناخته می‌شود، قابلیتی است که یک برنامه را قادر می‌سازد تا گفتار انسان را به فرمت نوشتاری پردازش کند. در حالی که معمولاً با تشخیص صدا اشتباه گرفته می‌شود، تشخیص گفتار بر ترجمه گفتار از فرمت کلامی به فرمت متنی تمرکز دارد، در حالی که تشخیص صدا فقط به دنبال شناسایی صدای یک کاربر منفرد است(IBM) .

منابع

Ambrozi, Austin. ”11 Challenges of Adopting AI In Business (And How To Address Them Head-On),” *Forbes*, October 24, 2023. https://www.forbes.com/sites/forbesbusinesscouncil/2023/10/24/11-challenges-of-adopting-ai-in-business-and-how-to-address-them-head-on/?sh=6710c8474bfe..

Ankers, Damon. “Types of Artificial Intelligence: A Detailed Guide.” *Certes IT Service Solutions*. https://certes..co..uk/types-of-artificial-intelligence-a-detailed-guide..

Appel, Gil; Juliana Neelbauer; David A. Schweidel. “Generative AI Has an Intellectual Property Problem.” *Harvard Business Review*, April 7, 2023. https://hbr..org/2023/04/generative-ai-has-an-intellectual-property-problem..

Billington, James. “The Prometheus Project: The Story Behind One of AV’s Greatest Developments.” *ADAS & Autonomous Vehicle International*, August 22, 2018. https://www..autonomousvehicleinternational..com/features/the-prometheus-project..html..

Britannica. “Artificial Intelligence.” *Encyclopedia Britannica*. 2023.. https://www..britannica..com/technology/artificial-intelligence..

Britannica. “Deep Blue Computer Chess-Playing System.” *Encyclopedia Britannica*. 2023.. https://www..britannica..com/topic/Deep-Blue..

COSO. “Guidance, Internal Control Integrated Framework.” *COSO*. 2023. https://www..coso..org/guidance-on-ic..

Deloitte. “Modernizing the three lines of defense model: An internal audit perspective.” Deloitte, 2023. https://www2..deloitte..com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model..html..

Doran, George T. “There’s a SMART Way to Write Management’s Goals and Objectives.” Management Review, 70, November 1981, 35-36. https://community.mis..temple..edu/mis0855002fall2015/files/2015/10/S..M..A..R..T-Way-Management-Review..pdf..

EY. “The CEO Outlook Pulse – October 2023,” EY, 2023. https://www..ey..com/en_us/ceo/ceo-outlook-global-report#:~:text=The%20CEO%20Outlook%20Pulse%20

Gartner. “Gartner Glossary.” Gartner. 2023.. https://www.. gartner..com/en/information-technology/glossary/cpu-central-processing-unit..

Hsu, Hansen. “Meet 2021 CHM Fellow Honoree Raj Reddy.” Computer History Museum. https://

computerhistory..org/blog/meet-2021-chm-fellow-honoree-raj-reddy/..

Humanoid Robotics Institute. “History of Humanoid Robot in Waseda University.” Waseda University. https://www..humanoid..waseda..ac..jp/history..html..

IBM. “eBook: Build responsible AI workflows with AI governance.” IBM. https://www..ibm..com/account/reg/ us-en/signup?formid=urx-51898..

IBM. “IBM Global AI Adoption Index.” IBM, 2023. https:// www..ibm..com/watson/resources/ai-adoption..

IBM. “Understanding the Different Types of Artificial Intelligence.” IBM, October 2023. https://www..ibm..com/ blog/understanding-the-different-types-of-artificial-intelligence/..

The Institute of Internal Auditors. CRMA Study Guide and Practice Questions, 3rd Edition. The IIA. 2023.. https://www..theiia..org/en/products/bookstore/crma-study-guide-and-practice-questions-3rd-edition/..

The Institute of Internal Auditors. Global Perspectives & Insights: The Artificial Intelligence Revolution. The IIA. 2023.. https://www..theiia..org/en/content/articles/ global-perspectives-and-insights/2023/global-perspectives-insights-the-artificial-intelligence-revolution/..

The Institute of Internal Auditors. The IIA's Three Lines Model: An update of the Three Lines of Defense. The IIA. 2020.. https://www..theiia..org/en/content/position-papers/2020/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense/?msclkid=f2923355c01e

The Institute of Internal Auditors. International Professional Practices Framework. 2017 ed. (Lake Mary, FL: The Institute of Internal Auditors, 2017). https:// www..theiia..org/en/products/bookstore/international-professional -practices-framework---ippf---2017-edition/..

Intel. "What is a GPU?" Intel. https://www..intel..com/ content/www/us/en/products/docs/processors/what-is-a-gpu..html..

ISACA. "COBIT, An ISACA Framework." ISACA. 2023.. https://www..isaca..org/resources/cobit..

ISACA. "Glossary." ISACA. 2022.. https://www..isaca..org/ resources/glossary..

Marr, Bernard. "The 15 Biggest Risks of Artificial Intelligence." Forbes. June 2, 2023. https://www..forbes.. com/sites/bernardmarr/2023/06/02/the-15-biggest-risks-of-artificial-intelligence/?sh=16756d8b2706..

McCarthy, J; M.L. Minsky; N. Rochester; C.E. Shannon. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence." BibSonomy. https://www..bibsonomy..org/ bibtex/24550126962fd8014daa80db1ffae4df2/ mhwombat..

Moyer, Steven; Gunter Brunhart; Richard Dubs, Thomas Erickson, Robert Skalamera, Rob Kepner, Marty Meyer, "A (Kind of) Quantitative Approach to Organizational Risk Tolerance." ISACA, July 8, 2021. https://www..isaca.. org/resources/news-and-trends/isaca-now-blog/2021/ a-kind-of-quantitative-approach-to-organizational-risk-tolerance..

National Cyber Security Centre. "Guidelines for secure AI system development." National Cyber Security Centre. 2023.. https://www..ncsc..gov..uk/collection/ guidelines-secure-ai-system-development..

NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0), Gaithersburg, Md..: NIST, 2023. https:// nvlpubs.nist.gov/nistpubs/ai/nist..ai..100-1..pdf..

NIST Computer Security Resource Center. "Glossary." Gaithersburg, Md..: NIST. https://csrc..nist..gov/glossary..

PwC. "PwC 2022 AI Business Survey (U..S..)." PwC. https:// www..pwc..com/us/en/tech-effect/ai-analytics/ai-business-survey..html..

QuantumBlack AI by McKinsey. "The State of AI in 2023: Generative AI's Breakout Year." McKinsey. 2023.. https://www..mckinsey..com/capabilities/

quantumblack/our-insights/the-state-of-ai-in-2023-generative-AIs-breakout-year..

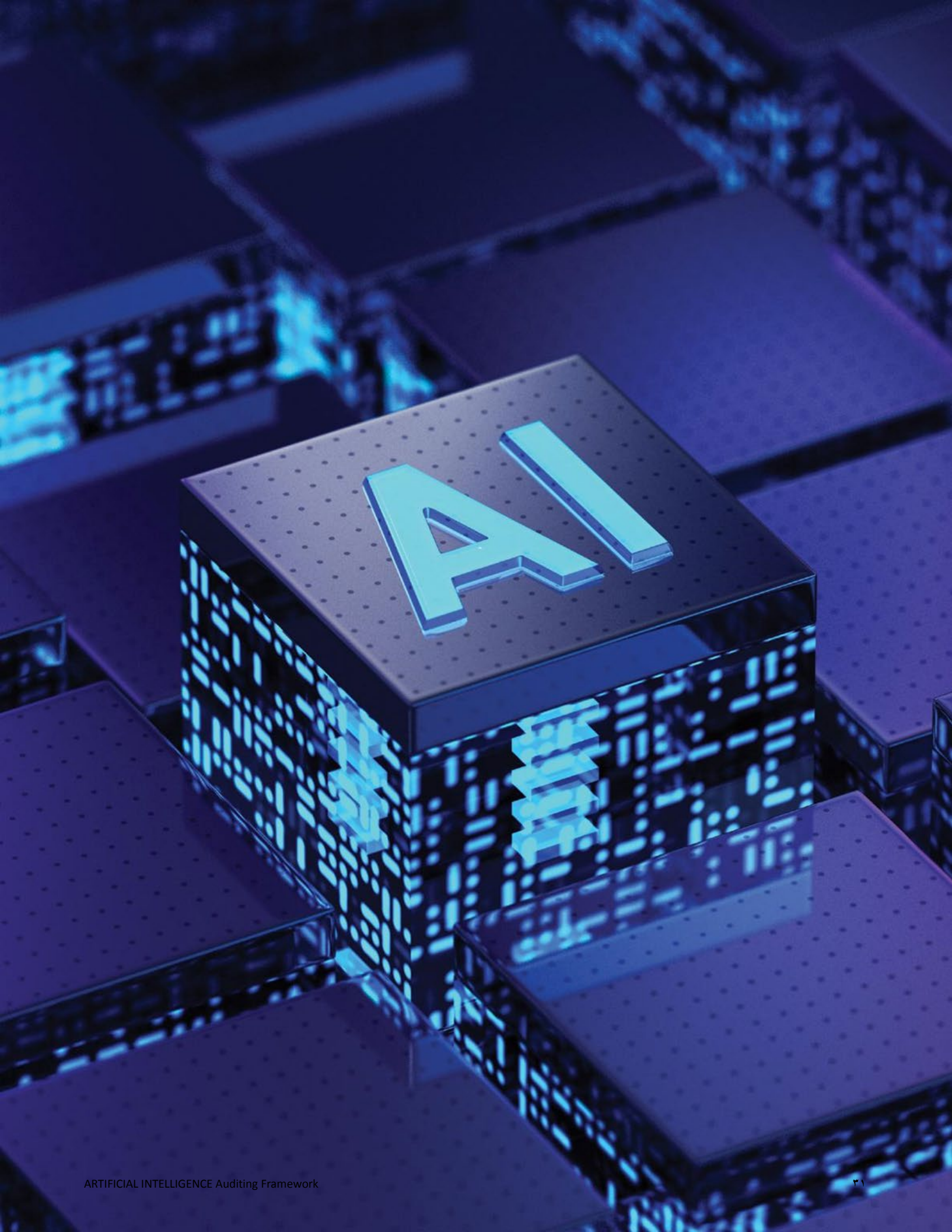
Samuel, A.L. "Some Studies in Machine Learning Using the Game of Checkers." IBM Journal of Research and Development. July 1959. https://ieeexplore..ieee..org/ document/5392560..

Techopedia.com. "TechDictionary." https://www.. techopedia..com/dictionary..

Turing, A.M. "Computing Machinery and Intelligence." Mind, Volume LIX, Issue 236, October 1950, Pages 433–460. https://academic..oup..com/mind/article/ LIX/236/433/986238..

Weizenbaum, Joseph. "ELIZA—A Computer Program for the Study of Natural Language Communication Between Man and Machine." Communications of the Association for Computing Machinery. January 1966. https://dl..acm..org/doi/10..1145/365153..365168..

White House. "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." The White House. October 30, 2023. https://www..whitehouse..gov/briefing-room/ statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/..


AI

Framework Development Team

George Barham, Allison Banzon, Anne Mercer, Kat Seeuws, Geoff Nordhoff.

Contributors

Andrew Cook, Pam Stroebel Powers, Robert Perez, Jim Enstrom, Scott Moore.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 245,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit **theiia.org**..

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

IIA Global Headquarters
[illegible]

The Institute of Internal Auditors