

راهنمای جامع حکمرانی داده

افراد، فرایندها و ابزارهای رسیدن به داده‌های مورد اعتماد

نویسندگان:

اورن اریورک

اوری گیلاد

والیپا لاکشمان

آنیثا کیبونگوچی گرنٹ

جسی آشداون

مترجمان:

بهزاد سجادی

امین هاشمی

عنوان و نام پدیدآور	راهنمای جامع حکمرانی داده (افراد، فرایندها و ابزارهای رسیدن به داده‌های مورد اعتماد) نویسندگان اورن اریورک ... (و دیگران)؛ مترجمان بهزاد سجادی، امین هاشمی.
مشخصات نشر	تهران: مهکامه، ۱۴۰۳.
مشخصات ظاهری	۲۷۲ ص: مصور، جدول.
شابک	۹۷۸-۶۲۲-۵۹۲۳-۴۷-۸
وضعیت فهرست‌نویسی	قیفا
یادداشت	عنوان اصلی: Data governance: the definitive guide: people, processes, and tools to operationalize data .trustworthiness, [2021].
یادداشت	کتاب حاضر نخستین بار با عنوان «حکمرانی داده‌ها: راهنمای قطعی افراد، فرایندها و ابزارها برای عملیاتی کردن اعتمادپذیری به داده‌ها» با مترجمان رامین مولاناپور، حمیدرضا فلاح کتک لاهیجانی توسط انتشارات آتی‌نگر سال ۱۴۰۳ قیفا گرفته است.
عنوان دیگر	حکمرانی داده‌ها: راهنمای قطعی افراد، فرایندها و ابزارها برای عملیاتی کردن اعتمادپذیری به داده‌ها.
موضوع	حفاظت داده‌ها Data protection
موضوع	مجموعه داده‌ها Data sets
موضوع	رایانش ابری Cloud computing
شناسه افزوده	اریورک، اورن Eryurek, Evren
شناسه افزوده	سجادی، بهزاد، ۱۳۶۶-، مترجم
شناسه افزوده	هاشمی، امین، ۱۳۶۷-، مترجم
رده‌بندی کنگره	HF۵۵۲۸۳۷
رده‌بندی دیویی	۶۵۸/۴۷۸
شماره کتابشناسی ملی	۹۹۵۱۴۳۳



انتشارات مهکامه

نام کتاب: راهنمای جامع حکمرانی داده (افراد، فرایندها و ابزارهای رسیدن به داده‌های مورد اعتماد)
 مؤلفان: اورن اریورک، اوری گیلاد، والیپا لاکسمان، آفتا کیبونگوچی گرت، جسی آشداون
 مترجمان: بهزاد سجادی، امین هاشمی
 ناشر: مهکامه

ناظر چاپ: بهزاد ربیعی فراهانی

طرح جلد: محمودرضا لطیفی

لیتوگرافی: نقش

نوبت چاپ: اول / ۱۴۰۴

تیراژ: ۳۰۰ نسخه

قیمت: ۳۲۰۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۵۹۲۳-۴۷-۸

کلیه حقوق چاپ و نشر این کتاب مطابق با «قانون حقوق مؤلفان و مصنفان مصوب ۱۳۴۸» برای ناشر محفوظ و منحصراً متعلق به نشر مهکامه می‌باشد. لذا هر گونه استفاده از کل یا قسمتی از این کتاب (از قبیل هر نوع چاپ، فتوکپی، اسکن، عکس‌برداری، نشر الکترونیکی، هر نوع انتشار بصورت اینترنتی، سی‌دی، دی‌وی‌دی، فیلم، فایل صوتی یا تصویری و غیره) بدون اجازه کتبی از نشر مهکامه ممنوع بوده و متخلفین تحت پیگرد قانونی قرار می‌گیرند.

انتشارات مهکامه

نشر و پخش: تهران، خیابان انقلاب، خیابان فخر رازی، نرسیده به لبافی‌نژاد، کوچه انوری، پلاک ۸، طبقه دوم

فکس: ۶۶۹۶۱۵۰۹

تلفن: ۶۶۶۸۸۲۰۳-۶۶۴۹۷۰۵۰-۶۶۹۶۱۵۰۹

واتساپ: ۰۹۰۳۲۶۷۴۸۴۴

همراه: ۰۹۱۲۳۹۷۴۰۲۱

www.mahkameh.com

اصلاحات و الحاقات احتمالی، در سایت انتشارات مهکامه:

en_mahkame@yahoo.com

پست الکترونیکی:

telegram.me/mahkamepublisher

تلگرام:

تخصص و جایگاه سازمانی نویسندگان در ابر گوگل

اورن اریورک

رهبر سبد تحلیل داده و مدیریت داده

اوری گیلا

راهبر حکمرانی داده و کلان داده

والیپا لاکشمان

مدیر راهکارهای تحلیل داده و هوش مصنوعی

آنیتا کیبونگوچی گرن

راهبر بازاریابی محصول مدیریت داده

جسی آشداون

محقق تجربه کاربری

www.ketab.ir

فهرست

پیش‌گفتار ۱۷

مقدمه مترجمان ۱۹

مقدمه نویسندگان ۲۱

چرا کسب‌وکارها به حکمرانی داده در محیط ابری نیاز دارند؟ ۲۳

چارچوب‌ها و بهروش‌ها برای حکمرانی داده در محیط ابری ۲۴

چارچوب حکمرانی داده ۲۴

عملیاتی‌سازی حکمرانی داده در سازمان ۲۷

منافع کسب‌وکاری حکمرانی قوی داده ۲۸

این کتاب برای چه کسانی مفید است؟ ۲۹

قراردادهای استفاده شده در کتاب ۳۰

فصل ۱: حکمرانی داده چیست؟ ۳۱

حکمرانی داده شامل چه مواردی است؟ ۳۲

نگرش جامع به حکمرانی داده ۳۵

افزایش اعتماد در داده‌ها ۳۶

طبقه‌بندی و کنترل دسترسی ۳۷

حکمرانی داده در مقایسه با توانمندسازی و امنیت داده‌ها ۳۹

چرا حکمرانی داده تا این حد مهم شده است؟ ۴۱

حجم داده‌ها در حال افزایش است ۴۱

تعداد افرادی که با داده‌ها کار کرده یا آن‌ها را مشاهده می‌کنند رشد نمایی داشته است ۴۲

روش‌های جمع‌آوری داده‌ها پیشرفت کرده است ۴۲

در حال حاضر انواع مختلف داده (شامل داده‌های حساس) جمع‌آوری می‌شود ۴۵

۴۶	موارد کاربرد داده گسترش یافته است
۴۹	قوانین و مقررات جدید در مورد نحوه رفتار با داده‌ها
۴۹	ملاحظات اخلاقی در ارتباط با استفاده از داده‌ها
۵۱	مثال‌هایی از حکمرانی داده در عمل
۵۱	مدیریت قابلیت اکتشاف، امنیت و مسئولیت‌پذیری
۵۲	افزایش کیفیت داده‌ها
۵۷	ارزش کسب‌وکاری حکمرانی داده
۵۷	پرورش نوآوری
۵۸	چالش میان حکمرانی داده و دموکراتیک کردن داده
۵۹	مدیریت ریسک (سرقت، سوءاستفاده، خرابی داده)
۶۱	انطباق با قوانین و مقررات
۶۴	ملاحظات سازمان‌ها در مورد حکمرانی داده‌ها
۶۶	چرا حکمرانی داده در ابر عمومی آسان‌تر است؟
۶۷	موقعیت مکانی داده‌ها
۶۸	کاهش سطح حکمرانی
۶۹	محاسبات موقت
۶۹	رایانش بدون سرور و قدرت
۷۰	منابع برچسب‌گذاری شده
۷۱	امنیت در دنیای هیبرید
۷۲	خلاصه

فصل ۲: ابزارها ۷۳

۷۳	دیکشنری سازمان
۷۴	کلاس‌های داده
۷۶	کلاس‌های داده و سیاست‌ها
۷۹	طبقه‌بندی و سازماندهی داده
۸۰	فهرست‌بندی داده و مدیریت فراداده
۸۱	ارزیابی و تهیه پروفایل داده‌ها
۸۲	کیفیت داده
۸۳	تبارشناسی داده

۸۴	مدیریت کلید و رمزنگاری
۸۷	نگهداری و حذف داده‌ها
۸۹	جریان کاری دستیابی به داده‌ها
۸۹	مدیریت هویت و دسترسی
۹۱	مجوزها و مدیریت دسترسی کاربران
۹۲	خلاصه

فصل ۳: افراد و فرایندها

۹۳	افراد، نقش‌ها، مسئولیت‌ها و کلاه آن‌ها
۹۴	تعریف کلاه‌ها
۱۰۱	غنی‌سازی داده‌ها و اهمیت آن
۱۰۲	فرایندها: سازمان‌ها، نیازمندی‌ها و رویکردهای مختلفی در ارتباط با حکمرانی داده دارند
۱۰۲	سازمان‌های قدیمی یا سنتی
۱۰۳	سازمان‌های تمام دیجیتال / مبتنی بر ابر
۱۰۴	خرده‌فروش‌ها
۱۰۶	سازمان‌های تحت نظارت قوی قانون
۱۰۹	سازمان‌های کوچک
۱۰۹	سازمان‌های بزرگ
۱۱۱	افراد و فرایندها: ملاحظات، نکته‌ها و برخی استراتژی‌های موفق
۱۱۱	ملاحظات و مسائل
۱۱۶	فرایندها و استراتژی‌های موفق اما متفاوت
۱۲۳	خلاصه

فصل ۴: حکمرانی داده در چرخه حیات داده

۱۲۵	چرخه حیات داده چیست؟
۱۲۶	فازهای چرخه حیات داده
۱۲۷	ایجاد داده
۱۲۸	پردازش داده
۱۲۸	ذخیره‌سازی داده
۱۲۹	استفاده از داده

۱۲۹		بایگانی داده
۱۳۰		از رده خارج کردن داده‌ها
۱۳۰		مدیریت چرخه حیات داده
۱۳۱		برنامه مدیریت داده
۱۳۳		اعمال حکمرانی در چرخه حیات داده
۱۳۳		چارچوب حکمرانی داده
۱۳۵		حکمرانی داده در عمل
۱۳۸		مثالی از نحوه حرکت داده‌ها داخل چارچوب
۱۴۲		عملیاتی‌سازی حکمرانی داده
۱۴۲		سیاست حکمرانی داده چیست؟
۱۴۳		اهمیت سیاست حکمرانی داده
۱۴۴		تدوین سیاست‌های حکمرانی داده
۱۴۵		ساختار سیاست حکمرانی داده
۱۴۶		نقش‌ها و مسئولیت‌ها
۱۴۷		راهنمای گام به گام
۱۵۰		ملاحظات در ارتباط با حکمرانی داده در چرخه حیات آن
۱۵۳		خلاصه

۱۵۵		فصل ۵: بهبود کیفیت داده
۱۵۵		کیفیت داده چیست؟
۱۵۶		چرا کیفیت داده مهم است؟
۱۵۹		کیفیت داده در تحلیل کلان داده‌ها
۱۶۰		کیفیت داده در مدل‌های یادگیری ماشین و هوش مصنوعی
۱۶۳		چرا کیفیت داده بخشی از برنامه حکمرانی داده است؟
۱۶۳		تکنیک‌هایی برای افزایش کیفیت داده
۱۶۵		کارت امتیازی
۱۶۶		اولویت‌بندی
۱۶۶		حاشیه نویسی
۱۶۷		ایجاد پروفایل
۱۷۴		خلاصه

فصل ۶: حکمرانی داده‌های در حال حرکت..... ۱۷۵

- ۱۷۵..... تبدیل داده.....
- ۱۷۷..... تبار داده.....
- ۱۷۷..... چرا تبار داده مفید است؟.....
- ۱۷۸..... چگونه تبار داده‌ها را جمع‌آوری کنیم؟.....
- ۱۷۸..... انواع تبار داده‌ها.....
- ۱۸۱..... بعد چهارم.....
- ۱۸۱..... چگونگی حکمرانی داده‌های در حال حرکت.....
- ۱۸۴..... مدیریت سیاست‌ها، شبیه‌سازی، پایش و مدیریت تغییر.....
- ۱۸۴..... ممیزی و انطباق.....
- ۱۸۵..... خلاصه.....

فصل ۷: حفاظت از داده‌ها..... ۱۸۷

- ۱۸۷..... برنامه‌ریزی حفاظت از داده‌ها.....
- ۱۸۸..... تبار و کیفیت.....
- ۱۸۹..... سطوح حفاظت.....
- ۱۹۰..... طبقه‌بندی.....
- ۱۹۱..... حفاظت از داده‌ها در محیط ابری.....
- ۱۹۱..... استفاده از منابع محاسباتی مشترک.....
- ۱۹۲..... سطح مستعد امنیت.....
- ۱۹۳..... امنیت ماشین‌های مجازی.....
- ۱۹۴..... امنیت فیزیکی.....
- ۱۹۶..... امنیت شبکه.....
- ۱۹۷..... امنیت در انتقال داده‌ها.....
- ۱۹۹..... جابجایی غیرمجاز داده.....
- ۲۰۲..... کنترل‌کننده‌های مجازی سرویس ابر اختصاصی.....
- ۲۰۴..... کد امن.....
- ۲۰۵..... مدل بی‌اعتمادی.....
- ۲۰۶..... مدیریت هویت و دسترسی.....
- ۲۰۶..... احراز هویت.....

۲۰۷.....	اعطای مجوز.....
۲۰۸.....	سیاست‌ها.....
۲۱۰.....	جلوگیری از فقدان داده‌ها.....
۲۱۱.....	رمزنگاری.....
۲۱۳.....	استفاده از اطلاعات کاربران بدون نقض حریم خصوصی آنان.....
۲۱۴.....	شفافیت دسترسی.....
۲۱۵.....	چابکی در محافظت از داده‌ها.....
۲۱۵.....	تحلیل‌های سلامت امنیت.....
۲۱۶.....	تبارشناسی داده.....
۲۱۶.....	شناسایی تهدیدها.....
۲۱۷.....	بهروش‌های محافظت از داده‌ها.....
۲۱۸.....	طراحی شبکه‌های مجزا.....
۲۱۸.....	امنیت فیزیکی.....
۲۲۰.....	سیاست‌ها و رمزنگاری ابزارهای قابل حمل.....
۲۲۰.....	فرایند حذف داده‌ها.....
۲۲۳.....	خلاصه.....

فصل ۸: پایش..... ۲۲۵

۲۲۵.....	پایش چیست؟.....
۲۲۶.....	چرا باید پایش انجام دهیم؟.....
۲۲۹.....	چه چیزی را پایش کنیم؟.....
۲۲۹.....	پایش کیفیت داده.....
۲۳۱.....	پایش تبار داده‌ها.....
۲۳۳.....	پایش انطباق.....
۲۳۴.....	پایش عملکرد برنامه حکمرانی داده.....
۲۳۶.....	پایش امنیت.....
۲۳۸.....	سیستم پایش چیست؟.....
۲۳۹.....	تحلیل بلادرنگ.....
۲۳۹.....	هشدارهای سیستمی.....
۲۳۹.....	اعلان‌ها.....

۲۳۹	 گزارش/تحلیل
۲۴۰	 مصورسازی
۲۴۰	 ویژه سازی
۲۴۱	 معیارهای پایش
۲۴۲	 یادآوری ها و نکات مهم
۲۴۳	 خلاصه

فصل ۹: ایجاد فرهنگ حفاظت از حریم خصوصی و امنیت

۲۴۵	 فرهنگ داده چیست و چرا مهم است؟
۲۴۶	 شروع از بالاترین سطح
۲۴۷	 تحلیل ها، درآمد و سود خالص سازمان
۲۴۷	 شخصیت و ادراک سازمان
۲۴۸	 اهداف، آموزش و ارتباطات
۲۴۹	 فرهنگ داده باید بر مبنای هدف باشد
۲۵۰	 آموزش: چه کسی، باید چه چیزی را بداند؟
۲۵۲	 فراتر از سواد داده
۲۵۲	 انگیزه و آثار متعاقب آن
۲۵۳	 حفظ و تداوم چابکی
۲۵۴	 نیازمندی ها، قوانین، مقررات و انطباق
۲۵۵	 اهمیت ساختار داده
۲۵۶	 افزایش یا کاهش مقیاس حکمرانی
۲۵۶	 تعامل با مسائل حقوقی و امنیتی
۲۵۶	 تسلط بر قوانین و مقررات
۲۵۷	 ارتباطات
۲۵۷	 تعامل در عمل
۲۵۸	 چابکی، کلید حل مساله
۲۵۸	 مدیریت رخدادها
۲۵۸	 وقتی همه مسئول باشد، در واقع هیچ کس مسئول نیست
۲۵۹	 اهمیت شفافیت
۲۵۹	 شفافیت به چه معناست؟

۲۶۰	اعتمادسازی درون سازمان.....
۲۶۰	اعتمادسازی خارج از سازمان.....
۲۶۱	ایجاد مثال.....
۲۶۱	خلاصه.....

ضمیمه ۱: حکمرانی داده در گوگل..... ۲۶۳

۲۶۳	طرح کسب و کار حکمرانی داده گوگل.....
۲۶۴	مقیاس حکمرانی داده گوگل.....
۲۶۵	فرایند حکمرانی داده گوگل.....
۲۶۷	گوگل چگونه داده‌ها را مدیریت می‌کند؟.....
۲۶۷	حریم خصوصی امن - مورد کاوی ADH.....

ضمیمه ۲: منابع مطالعاتی اضافی..... ۲۷۱

۲۷۱	فصل ۴: حکمرانی داده در چرخه حیات داده.....
۲۷۲	فصل هشتم: پایش.....

شرکت دانش آفرینان نیک اندیش (دیجی وایز) همواره تلاش نموده است دانش روز دنیا را به کشور منتقل نماید. زمانی دیجی وایز بر تحول فناوری اطلاعات و ارتباطات متمرکز بود و در این مسیر تعامل بسیار موافی با شرکت‌های بزرگ دنیا داشت و توانست متدلوژی و نظام‌های روز دنیا جهت تحول فناوری اطلاعات را به کشور منتقل نماید. در ادامه با ظهور پدیده تحول دیجیتال تبدیل به اولین شرکتی در ایران شد که با استفاده از یک متدلوژی معتبر بین‌المللی، طرح تحول دیجیتال را برای یکی از بزرگترین بانک‌های کشور تدوین نمود.

با توسعه مفاهیم مرتبط با مدیریت تجربه مشتریان، رویکردی ساخت‌یافته در طراحی و استقرار نظام مدیریت تجارب مشتریان مبتنی بر رویکرد یک شرکت معتبر بین‌المللی مشاوره مدیریت طراحی و اولین پروژه بازطراحی محصولات و رویکرد ارائه خدمات مبتنی بر تجربه مشتریان را در کشور اجرایی نمود.

در این مسیر یکی از حوزه‌های کلیدی که مدتی است در جهان به عنوان یک دانش بسیار مهم جلب توجه کرده است استراتژی و حاکمیت داده می‌باشد. دیجی وایز موفق گردید اولین پروژه تدوین استراتژی و طراحی نظام حاکمیت داده را مبتنی بر یک متدلوژی نوین بین‌المللی برای یکی از بانک‌های معتبر کشور تدوین نماید. از آنجایی که دیجی وایز، نشر دانش و توسعه مهارت‌های مدیران و متخصصین کشور را جزء مسئولیت‌های خود می‌داند و مشاهدات ما نشان می‌داد که دانش حوزه حاکمیت داده در کشور محدود است بر آن شدیم تا یکی از معتبرترین منابع دنیا در این حوزه را توسط دو تن از برترین متخصصین خود به فارسی ترجمه نماییم. امید است در راستای اعتلای دانش کشور موثر واقع گردد.

مقدمه مترجمانی

در مسیر تعالی حرفه‌ای و کسب تخصص رویکردهای مختلفی وجود دارد که رجوع به دانش مستند در قالب کتاب و مقالات روشی دیرینه است. در این بین، اصالت مرجع دانش اهمیت بسزایی دارد و اخذ آن اصطلاحاً از مرجع دست اول باعث می‌شود، دانش با کمترین ریزش به مخاطب منتقل شود. سرلوحه ما در کسب دانش و تخصص همواره این بوده که در دنیای فناوری، به ویژه دیجیتال و به‌طور خاص داده، کشورها، سازمان‌ها و افراد بسیار پیشرویی وجود دارند. مادامی که آنان در حوزه‌های پیشرو دانش تولید می‌کنند، احتیاط واجب آن است که اکتساب ما نیز از منبع اصلی باشد، لذا در حیطه این کتاب، ترجمه را بر تالیف مقدم می‌دانیم.

از طرفی، اکنون و در زمان ترجمه این کتاب امیدهای بسیاری به هوش مصنوعی وجود دارد، در منحنی هایپ گارتنر انتظارات از هوش مصنوعی مولد در بالاترین سطح خود قرار دارد و همگان، از متخصصان و فعالان حرفه‌ای تا افشار مختلف جامعه در هر حوزه‌ای به ابزارهای این دستاورد مهم بشریت پناه می‌برند. در حوزه تولید محتوا و اخص ترجمه نیز سرعت، سهولت، فراگیری و حجم تولیدات مبتنی بر ابزارهای آنلاین هوشمند قابل توجه است و باید سخن کوتاه کرده و اذعان کنیم که در این عصر ترجمه و چاپ کتاب فضیلت خاصی برای مترجمان و ناشران محسوب نمی‌شود و چه بسا امری بیهوده تلقی شود.

اما با هدف اکتساب دانش از منبعی اصلی و برای ترجمه این اثر به ابعادی فارغ از وضعیت مذکور توجه داشتیم. امروزه در کشور ما متخصصان همچون سراسر دنیا به حوزه داده به عنوان عنصر یکپارچه‌ساز برای تحقق دنیای دیجیتال توجه ویژه‌ای دارند، متخصصان ارزشمندی در این حوزه در حال فعالیت هستند و در کوران مهاجرت غمناک عزیزانمان، هنوز فقدان محتوایی ساختارمند برای تربیت نظام‌مند متخصصان جدید به شدت احساس می‌شود.

تجربه چندین سال فعالیت در سازمان‌های بزرگ و پیشرو در زیست‌بوم دیجیتال کشور بر ما آشکار کرد که هنوز در تبیین و انتقال بسیاری از مفاهیم حوزه داده به ارکان مختلف سازمان، زبانی الکن داریم چرا که مفاهیم نوظهور هر آن در حال زایش و پالایش هستند و در

این بین برداشت‌های مختلف، ذهنیت‌های متنوع را حتی در مفاهیم پایه‌ای، ایجاد کرده است.

و در نهایت به همان دلایلی که ذکر شد، در این مقدمه برای آن‌که ارزشی فراتر از ماشین‌ها، فراهم کنیم سعی کردیم در عین امانتداری نسبت به متن به‌طور یک‌ه مفاهیم مفقود نشوند، برگردان‌های مناسب و متناسبی برای واژگان انتخاب کنیم که برای خوانندگان فارسی زبان فعال در اکوسیستم دیجیتال کشور مانوس باشد. از طرفی هم توضیحات اضافی و تبیین‌های بیشتری را در جای جای کتاب شامل متن اصلی و پانویس‌ها اضافه کردیم. با این امید که در پایان مطالعه این کتاب مفاهیم به‌صورت ساختارمند در ذهن خوانندگان رسوب کند.

ما به نقصان‌های ممکن‌مان در حوزه دانش فنی علم داده، زبان و ادبیات فارسی و فن ترجمه آگاهیم و با کمال میل از خوانندگان عزیز تقاضا داریم با بازخوردهای سازنده‌شان که به هر طریق، چه در دیدارهای حضوری و چه از طریق شبکه‌های اجتماعی حاصل شود، ما را در بهبود مستمر یاری کرده و در ارتقای کیفیت آثار بعدی سهیم باشند.

بهزاد سجادی

امین هاشمی

زمستان ۱۴۰۳

برای بهاری مانا

www.ketab.ir

مقدمه نویسنده گان

در سال های اخیر، سهولت انتقال به فضای ابری عاملی انگیزشی و انرژی بخش برای جامعه ای رو به رشد از مصرف کنندگان داده ها به منظور جمع آوری، ذخیره سازی و تحلیل داده ها در راستای ایجاد بینش و تصمیم گیری شده است. به دلایل مختلف، همانطور که اتخاذ رویکرد پردازش ابری توسعه می یابد، سوالاتی برای ذینفعان مدیریت اطلاعات در ارتباط با ریسک های بالقوه مرتبط با مدیریت داده ها در محیط ابری به وجود می آید. اورن¹ (یکی از نویسندگان کتاب) برای اولین بار، هنگامی که در صنعت سلامت کار می کرد به چنین سوالاتی مواجه و مجبور شد فرایندها و ابزارهایی را برای حکمرانی داده ها به کار گیرد. در حال حاضر در ابر گوگل، اوری² و لک³ (نویسندگان دیگر کتاب) تقریباً هر هفته به چنین سوالاتی پاسخ می دهند و در ارتباط با مواردی مانند ارزش آفرینی از داده، شکستن سیلوهای داده، حفظ ناشناس بودن، محافظت از اطلاعات حساس و بهبود قابل اعتماد بودن داده ها مشاوره می دهند.

ما متوجه شدیم GDPR همان چیزی است که باعث تغییر رفتار مشتریان شده است. حتی بعضی از مشتریان داده های خود را حذف کرده بودند چون فکر می کردند کار درستی انجام می دهند. این عکس العمل بیش از هر چیزی ما را بر آن داشت تا با در نظر داشتن مشاوره هایی که سال ها به مشتریان ابر گوگل می دادیم، این کتاب را بنویسیم. اگر داده ارزش جدیدی باشد، ما نمی خواهیم که سازمان ها از آن بترسند. اگر داده قفل شده یا قابل اعتماد نباشد، ارزشی هم ندارد.

ما به خودمان افتخار میکنیم که به مشتریانمان کمک کردیم تا از هزینه های فنی ای که متحمل شده اند، ارزش خلق کنند. داده سرمایه ای عظیم است و ما خود را موظف می دانیم تا برای مشتریانمان بهترین مسیر برای خلق ارزش از آن را فراهم کنیم.

سوالات مشتریان معمولاً شامل یکی از سه فاکتور ریسک است:

1. Evren
2. Uri
3. Lak

◇ امن‌سازی داده

ذخیره‌سازی داده در زیرساخت ابری، ممکن است برای سازمان‌های بزرگ که عموماً سیستم‌ها را در محل خود و با در نظر گرفتن حداکثر امنیت مستقر می‌کنند، نگران‌کننده باشد. سازمان‌ها با توجه به تعداد زیاد تهدیدها و نقض‌های امنیتی‌ای که هر روز در اخبار اعلام می‌شود نگران می‌شوند که ممکن است قربانی بعدی باشند. این عوامل بخشی از مدیریت ریسک برای حفاظت از داده‌ها در مقابل دسترسی‌های غیرمجاز به داده‌های حساس اعم از اطلاعات شناسایی شخصی، اطلاعات محرمانه سازمانی، اسرار تجاری و مالکیت معنوی است.

◇ انطباق با قوانین و مقررات^۱

قوانین و مقررات در حوزه‌های مختلف در حال توسعه هستند. مانند GDPR، CCPA و برخی قوانین مختص صنایع مانند LEI، تعدادی در صنعت مالی و استاندارد داده ACORD در صنعت بیمه. تیم‌های انطباق به عنوان مسئول کنترل پای‌بندی به این استانداردها ممکن است نگرانی‌هایی در مورد نظارت و کنترل داده‌های ذخیره شده در محیط ابری داشته باشند.

◇ چشم‌انداز و کنترل

گاهی اوقات متخصصان مدیریت داده و همچنین مصرف‌کنندگان داده چشم‌اندازی از داده‌های خود ندارند: کدام دارایی‌های داده در دسترس هستند؟ در کجا قرار دارند و آیا می‌توان از آنها استفاده کرد؟ چگونه می‌توان از آنها استفاده نمود؟ چه کسی به داده‌ها دسترسی دارد و اصلاً باید دسترسی داشته باشد؟ این عدم قطعیت توانایی آنها را برای استفاده بیشتر از داده‌های خود در بهبود بهره‌وری یا هدایت ارزش کسب‌وکار محدود می‌کند.

این فاکتورهای ریسک به وضوح نیاز به افزایش ارزیابی داده‌ها، فهرست بندی فراداده^۲، مدیریت کنترل دسترسی، کیفیت داده‌ها و امنیت اطلاعات را به عنوان شایستگی‌های اصلی حکمرانی داده‌ها نشان می‌دهند. شایستگی‌هایی که ارائه‌دهنده زیرساخت ابری باید آن‌ها را ارائه کرده و همچنین به‌طور مداوم به‌صورت شفاف ارتقاء دهد. در اصل، پرداختن به این خطرات بدون چشم‌پوشی از مزایای ارائه شده توسط رایانش ابری، نه تنها اهمیت درک حکمرانی داده‌ها در محیط ابری را افزایش داده، بلکه دانستن موضوعات مهم را نیز بهبود بخشیده است. حکمرانی مناسب داده مشوقی برای اعتماد مشتری است و به بهبودهای بزرگی در تجربه مشتری منجر می‌شود.

چرا کسب و کارها به حکمرانی داده در محیط ابری نیاز دارند؟

هرچقدر که کسب و کار داده‌های بیشتری را تولید و به محیط ابری منتقل کند، پیچیدگی مدیریت داده‌ها نیز از ابعاد مختلف تغییر می‌کند. سازمان‌ها باید به موارد زیر توجه کنند:

♦ مدیریت ریسک

همیشه نگرانی‌هایی در مورد افشای اطلاعات حساس توسط افراد یا سیستم‌های غیرمجاز، نقض‌های امنیتی و کارکنانی که به اشتباه به داده‌ها دسترسی دارند وجود دارد. سازمان‌ها به دنبال به حداقل رساندن این خطرات هستند، بنابراین انواع حفاظت‌های بیشتر (مانند رمزنگاری) برای مبهم کردن اطلاعات تعبیه شده در موجودیت داده، به منظور محافظت از داده‌ها در صورت رخنه در سیستم مورد نیاز است. علاوه بر این، ابزارهای دیگری برای پشتیبانی از مدیریت دسترسی، شناسایی دارایی‌های داده‌ای حساس و ایجاد سیاست در مورد حفاظت از آنها نیز باید مورد توجه قرار گیرد.

♦ تکثیر داده^۱

سرعتی که کسب و کارها با آن دارایی‌های داده خود را ایجاد، به‌روزرسانی و جریان می‌دهند افزایش یافته است. با وجود این که پلتفرم‌های مبتنی بر ابر قادر به مدیریت افزایش سرعت، حجم و تنوع داده‌ها هستند، باید کنترل‌ها و مکانیزم‌هایی برای تأیید سریع کیفیت جریان‌های داده‌ای با پهنای باند بالا تعریف شوند.

♦ مدیریت داده

نیاز به استفاده از منابع و جریان‌های داده تولید شده خارج از سازمان (از جمله داده‌های اخذ شده از اشخاص ثالث) به این معنی است که باید آماده باشید تا به همه منابع خارجی داده اعتماد نکنید. ممکن است لازم باشد از ابزارهایی استفاده نمایید که فرایند تبارشناسی داده‌ها، طبقه‌بندی آنها و فراداده را مستند می‌کنند تا به کارکنان شما (به ویژه مصرف کنندگان داده) کمک کنند که بر اساس شناخت خود از نحوه تولید دارایی‌های داده، قابلیت استفاده از داده‌ها را تعیین کنند.

♦ قابلیت اکتشاف (و آگاهی از داده)

انتقال داده‌ها به هر نوع دریاچه داده (مبتنی بر ابر یا در محل سازمان) ریسک از دست دادن ردیابی دارایی‌های داده منتقل شده، ویژگی‌های محتوایی آنها و جزئیات مربوط به فراداده مرتبط با آنها را به همراه دارد. بنابراین توانایی ارزیابی محتوا و حساسیت دارایی‌های داده، صرف نظر از اینکه کجا نگهداری می‌شوند، اهمیت بسیار پیدا می‌کند.

◊ حریم خصوصی و انطباق با قوانین و مقررات

انطباق با قوانین و مقررات مستلزم استانداردها و رویه‌های قابل ممیزی و اندازه‌گیری است که انطباق با سیاست‌های داده‌ای درون سازمانی و همچنین قوانین و مقررات خارج از سازمان مانند دولت را تضمین می‌کند. انتقال داده‌ها به فضای ابری به این معنی است که سازمان‌ها به ابزارهایی برای اعمال نظارت و گزارش انطباق و همچنین اطمینان از دسترسی و مجوزهای افراد و سرویس‌های مجاز به داده‌ها، نیاز دارند.

چارچوب‌ها و بهروش‌ها برای حکمرانی داده در محیط ابری

با توجه به پویایی در حال تغییر مدیریت داده‌ها، سازمان‌ها چگونه باید در مورد حکمرانی داده در محیط ابری فکر کنند و چرا این موضوع مهم است؟ بر اساس تعریف تک تارگت^۱، حکمرانی داده عبارت است از:

مدیریت کلان در دسترس بودن، کاربردپذیری، یکپارچگی و امنیت داده‌های مورد استفاده در سازمان. برنامه صحیح حکمرانی داده شامل کمیته یا شورای حکمرانی داده، مجموعه‌ای از رویه‌های تعریف شده و برنامه‌ای برای اجرای آن رویه‌ها است.^۲

به زبان ساده، حکمرانی داده‌ها شامل روش‌هایی است که افراد، فرایندها و فناوری با همکاری یکدیگر، انطباق قابل صحت‌سنجی با سیاست‌های داده‌ای تعریف شده و مورد توافق قرار گرفته را فراهم می‌کنند.

چارچوب حکمرانی داده

سازمان‌ها باید درباره حکمرانی داده، از لحظه ورود و یافتن داده‌ها تا فهرست‌بندی، ماندگاری، نگهداری، مدیریت ذخیره‌سازی، به اشتراک‌گذاری، بایگانی، پشتیبان‌گیری، بازیابی، جلوگیری از فقدان و حذف دائمی و موقت آنها به صورت کاملاً جامع فکر کنند.

◊ اکتشاف و ارزیابی داده

اغلب اوقات محیط‌های مبتنی بر ابر، گزینه‌هایی اقتصادی برای ایجاد و مدیریت دریاچه داده پیشنهاد می‌دهند. اما ریسک مهاجرت بدون حکمرانی داده در جای خود باقی است. این ریسک حکایت از خطری بالقوه از حیث فقدان این موارد است که، کدام داده‌ها در دریاچه داده هستند؟ چه اطلاعاتی در هر موجودیت داده وجود دارد؟ و منشأ موجودیت‌های داده چیست؟ اکتشاف و

1. TechTarget

2. Craig Stedman and Jack Vaughan, "What Is Data Governance and Why Does It Matter?" TechTarget, December 2019

ارزیابی داده، بهروشی است برای حکمرانی داده در محیط ابری به منظور شناختن دارایی‌های داده‌ای که در اختیار داریم. فرایند اکتشاف و ارزیابی داده برای مشخص کردن دارایی‌های داده در محیط ابری، شامل رهگیری و ضبط منشا و تبار داده، تبدیل‌های اعمال شده روی داده و فراداده است (فراداده اغلب شامل جزئیاتی از اطلاعات هویتی مانند نام ایجاد کننده، اندازه داده‌ها، تعداد رکوردها در صورت ساختاریافته بودن موجودیت داده و زمان آخرین به‌روزرسانی است).

❖ طبقه‌بندی و سازماندهی داده

ارزیابی صحیح دارایی داده و اسکن محتوای ویژگی‌های مختلف آن به دسته‌بندی دارایی داده برای سازمان‌دهی کمک می‌کند. این فرایند همچنین به این نکته می‌رسد که آیا موجودیت داده دارای داده‌های حساس است و در این صورت داده را با توجه به سطح حساسیت آن در سطوحی مانند شخصی، خصوصی، محرمانه و مالکیت معنوی دسته‌بندی می‌کند. برای پیاده‌سازی حکمرانی داده‌ها در محیط ابری باید پروفایل داده‌های حساس را تهیه کرده و طبقه‌بندی کنید تا بدانید چه سیاست‌ها و رویه‌های حکمرانی‌ای را باید روی آنها اعمال کنید.

❖ فهرست‌بندی و مدیریت فراداده

باید هنگامی که دارایی‌های داده‌ای شما ارزیابی و طبقه‌بندی شدند نسبت به مستندسازی آموخته‌های خود اقدام کنید. در این صورت مصرف‌کنندگان داده، دید روشنی نسبت به دیدگاه سازمان در خصوص داده پیدا می‌کنند. باید کاتالوگ داده‌ای نگهداری کنید که شامل ساختار فراداده، موجودیت فراداده و ارزیابی سطوح حساسیت در رابطه با دستورالعمل‌های حکمرانی مانند انطباق با یک یا چند قانون در زمینه حفظ حریم خصوصی داده‌ها باشد. کاتالوگ داده‌ها نه تنها به مصرف‌کنندگان داده اجازه می‌دهد تا این اطلاعات را مشاهده کنند، بلکه به عنوان بخشی از نمایه‌ای معکوس برای جستجو و کشف، هم از طریق عبارت^۱ (با توجه به هستی‌شناسی مناسب) و هم بر اساس مفهوم^۲ عمل می‌کند. همچنین باید قالب موجودیت داده‌های ساختاریافته و نیمه ساختاریافته را درک کرده و به سیستم‌ها اجازه دهید تا در صورت لزوم این نوع داده‌ها را به‌طور متفاوت مدیریت کنند.

❖ مدیریت کیفیت داده

مصرف‌کنندگان مختلف داده‌ها، نیازمندی‌های مختلفی دارند. بنابراین باید ابزاری برای مستندسازی انتظارات از کیفیت داده‌ها و همچنین تکنیک‌ها و ابزارهایی برای پشتیبانی از فرایند صحت‌سنجی و پایش داده‌ها ارائه شود. فرایند مدیریت کیفیت داده شامل موارد زیر است: ایجاد کنترل‌هایی برای صحت‌سنجی داده‌ها، پایش و گزارش کیفیت داده‌ها، پشتیبانی از فرایند تریاز برای ارزیابی شدت

1. Phrase

2. Concept

رخدادها و رهگیری اتفاقات و حوادثی که روی داده‌ها رخ می‌دهد. فرایند صحیح مدیریت کیفیت داده‌ها، باعث ایجاد داده‌هایی قابل اعتماد و قابل اندازه‌گیری برای ارائه تحلیل‌های مختلف می‌شود.

۵ مدیریت دسترسی به داده‌ها

حکمرانی دسترسی به داده‌ها دارای دو جنبه است. یکی ایجاد دسترسی به داده‌های موجود و دیگری جلوگیری از دسترسی غیرمجاز به داده‌ها. در ارتباط با ایجاد دسترسی به داده‌ها باید به مصرف‌کنندگان داده دسترسی‌های لازم در قالب سرویسی برای دستیابی به داده‌هایشان اعطا شود. خوشبختانه محیط‌های ابری روش‌های مختلفی را برای ارائه این سرویس‌ها دارند. در ارتباط با جلوگیری از دسترسی غیرمجاز به داده‌ها، نکته مهم ایجاد موجودیت‌ها، گروه‌ها، نقش‌ها و اعطای دسترسی به آنها برای ایجاد مفهوم دسترسی مدیریت شده است. این به‌روش شامل ارائه سرویس‌های مدیریت دسترسی ضمن ارتباط با سرویس‌های احراز هویت و مدیریت دسترسی ارائه شده توسط محیط ابری است. این سرویس‌ها با مدیریت دسترسی و تخصیص کلید تضمین می‌کنند که افراد و سیستم‌های احراز هویت شده و مجاز بر اساس نقششان به داده‌ها دسترسی داشته باشند.

۵ ممیزی

سازمان‌ها باید سیستم‌هایشان را ارزیابی کنند تا از کارکردشان طبق آن‌چه که بدان منظور طراحی شده‌اند مطمئن شوند. قبل از آن‌که خطری برای کسی ایجاد شود، پایش^۱، ممیزی^۲ و ردیابی^۳ (چه کسی چه کاری را در چه زمانی و با استفاده از چه اطلاعاتی انجام می‌دهد) به تیم‌های امنیت برای جمع‌آوری داده‌ها، تشخیص تهدیدها و پاسخ به آنها کمک می‌کنند. بنابراین انجام ممیزی‌های منظم برای بررسی اثربخشی کنترل‌های ریسک به منظور کاهش سریع تهدیدات و ارزیابی سلامت کلی امنیت مهم است.

۵ حفاظت از داده‌ها

با وجود تلاش تیم‌های فناوری اطلاعات برای ایجاد امنیت محیطی به عنوان راهی برای جلوگیری از دسترسی‌های غیرمجاز به داده‌ها، این نوع امنیت هرگز برای حفاظت از داده‌های حساس کافی نیست. وقتی در جلوگیری از دسترسی غیرمجاز به سیستم‌ها اقدامی انجام می‌دهید، بدین معنی نیست که در مقابل خطرات داخلی، افشاء، دزدی و جابجایی غیرمجاز داده‌ها در امان هستید. بنابراین استفاده از روش‌های بیشتری مانند رمزنگاری کامل، رمزنگاری حین انتقال، پوشش داده‌ها^۴ و حذف دائمی داده‌ها برای حفظ امنیت از اهمیت بسیاری برخوردار است.

1. Monitoring
2. Auditing
3. Tracking
4. Data Masking

عملیاتی‌سازی حکمرانی داده در سازمان

قطعا فناوری از مواردی که در بخش قبل عنوان شد پشتیبانی می‌کند اما حکمرانی داده چیزی فراتر از استفاده از ابزارها است. موفقیت برنامه حکمرانی داده، وابسته به ترکیب موارد زیر است:

- افرادی برای تدوین طرح کسب‌وکار، توسعه مدل عملیاتی و برعهده گرفتن نقش‌های مناسب

- فرایندهایی برای عملیاتی‌سازی تدوین، توسعه و اعمال سیاست‌ها

- فناوری‌هایی برای سهولت اجرای فرایندها توسط افراد

برنامه‌ریزی، اجرا و پشتیبانی از برنامه حکمرانی داده طی گام‌های زیر انجام می‌شود:

۱- ایجاد طرح کسب و کار

ایجاد طرح کسب‌وکار با شناسایی محرک‌های مهم کسب‌وکار برای توجیه تلاش و سرمایه‌گذاری در حکمرانی داده. همچنین ترسیم نمای کلی از ریسک‌های مرتبط با داده‌ها (مانند ذخیره‌سازی داده‌ها در پلتفرم ابری) و نشان دادن این‌که حکمرانی داده چگونه برای کاهش این خطرات به سازمان کمک می‌کند.

۲- مستندسازی اصول راهنما

تدوین اصول مرتبط با حکمرانی و نظارت داده در سازمان و مستندسازی آن در قالب منشور حکمرانی داده برای ارائه به مدیریت ارشد

۳- درگیر کردن مدیریت

درگیر کردن قهرمانان مدیریت داده و ذینفعان کلیدی و ارشد. ارائه طرح کسب‌وکار و اصول راهنما به سطح مدیران ارشد برای دریافت تایید.

۴- ایجاد مدل عملیاتی

تعریف نقش‌ها و مسئولیت‌های حکمرانی داده و پس از آن، شرح فرایندها و رویه‌هایی برای کمیته حکمرانی داده و تیم‌های ناظران داده به منظور تعریف و پیاده‌سازی سیاست‌ها و بررسی و رفع مشکلات داده‌ای شناسایی شده.

۵- پیاده‌سازی چارچوب مسئولیت‌پذیری و پاسخگویی

پیاده‌سازی چارچوبی برای تخصیص داده‌بان‌ها^۱ و مسئولیت‌ها به دامنه‌های داده‌ای بسیار حیاتی. حصول اطمینان از اینکه مالک داده، دید روشنی از داده‌ها در سازمان دارد و ارائه روشی برای حصول اطمینان از اینکه همه برای مشارکت در کاربردپذیری داده‌ها مسئولیت دارند.

۶- گونه شناسی^۱ و هستی شناسی^۲

ممکن است بخشنامه‌های مختلفی درباره طبقه‌بندی، سازماندهی و حفاظت از داده‌ها- به خصوص در ارتباط با داده‌های حساس- وجود داشته باشد. برای قانع کردن مصرف‌کنندگان داده در ارتباط با این بخشنامه‌ها، باید شرح واضحی از دسته‌بندی‌ها (مطابق با ساختار سازمانی) و طبقات مختلف (برای ارزیابی حساسیت داده‌ها) وجود داشته باشد.

۷- کنار هم قرار دادن فناوری‌ها

پس از تخصیص نقش‌ها و مسئولیت‌ها به افراد و مشخص کردن و تایید روال‌ها و فرایندها، باید مجموعه‌ای از فناوری‌ها کنار یکدیگر قرار گیرند تا صحت‌سنجی و انطباق با سیاست‌ها و ارائه گزارش‌های تطبیقی دقیق را تسهیل کنند.

۸- آموزش

آگاهی‌افزایی در ارتباط با ارزش حکمرانی داده با استفاده از منابع آموزشی که تجارب و روال‌های مرتبط با حکمرانی داده در آن نقش پررنگی دارند و توسط فناوری نیز پشتیبانی می‌شوند. همچنین برنامه‌ریزی برای برگزاری جلسات آموزشی به صورت منظم برای تقویت شیوه‌های تجارب خوب حکمرانی داده.

منافع کسب و کاری حکمرانی قوی داده

امنیت، حفاظت، دسترس‌پذیری و کاربردپذیری، کیفیت و سایر جنبه‌های حکمرانی داده به عنوان مهمترین اولویت‌های مدیریت داده در سازمان‌ها پدیدار شده و رشد خواهند یافت. با مهاجرت سازمان‌ها به سمت استقرار داده‌ها در محیط ابری، نیاز به روش‌هایی برای اطمینان از کارایی داده‌ها نیز رشد خواهد کرد. برای رسیدگی به این موضوعات، سازمان‌ها باید شیوه‌های حکمرانی داده خود را حول سه مولفه کلیدی تنظیم کنند:

• چارچوبی برای توانمندسازی افراد در راستای تعریف، تصویب و اعمال سیاست‌های

حکمرانی داده

• فرایندهایی اثربخش برای کنترل، بینش و نظارت بر تمام دارایی‌های داده موجود در

سیستم‌های داخلی، محیط ذخیره‌سازی ابری و پلتفرم‌های ائبار داده

• ابزارها و فناوری‌های صحیح برای عملیاتی سازی انطباق با سیاست‌های حکمرانی داده

سازمان‌ها با در نظر گرفتن این چارچوب، استراتژی موثر حکمرانی داده و مدل عملیاتی منطبق با آن، مسیری را برای کنترل و داشتن بینش نسبت به دارایی‌های داده ایجاد می‌کند که مزیتی

رقابتی را نسبت به همتایان خود فراهم کنند. سازمان‌ها با ترویج فرهنگ داده‌محور، از مزایای بسیار زیادی برخوردار خواهند شد، مزایایی مانند:

♦ بهبود تصمیم‌سازی

بهبود اکتشاف داده‌ها به این معنی است که کاربران، داده‌ای را که می‌خواهند در زمانی که می‌خواهند پیدا می‌کنند و بدین ترتیب کارایی آنان بالاتر می‌رود. تصمیم‌سازی بر مبنای داده نقش غیرقابل انکاری در بهبود برنامه‌ریزی توسط سازمان ایفا می‌کند.

♦ مدیریت بهتر ریسک

مدل عملیاتی مناسب به سازمان‌ها کمک می‌کند که فرایندهای خود را به روش ساده‌تری ممیزی کنند و بدین ترتیب ریسک جریمه شدن کاهش پیدا کرده و اعتماد مشتریان و عملکرد سازمان نیز بهبود می‌یابد. ضمن افزایش کارایی، مدت زمان در دسترس نبودن سیستم‌ها نیز کمتر می‌شود.

♦ انطباق با قوانین و مقررات

روند رو به رشد وضع قوانین و مقررات دولتی، اهمیت ایجاد راهکارهای حکمرانی داده را در سازمان‌ها بالا برده است. با استفاده از چارچوب مناسب حکمرانی داده، سازمان‌ها می‌توانند به جای اینکه صرفاً به تغییرات قانونی و نظارتی واکنش نشان دهند، از آن استقبال کرده و آنرا بپذیرند. هنگامی که داده‌ها را به محیط ابری منتقل می‌کنید، حکمرانی داده سطحی از حفاظت را برای اجتناب از استفاده نامناسب از داده‌ها ایجاد می‌کند. در عین حال، انطباق قابل ممیزی با سیاست‌های داده‌ای تعریف‌شده کمک می‌کند تا به مشتریان خود نشان دهید که از اطلاعات خصوصی آن‌ها محافظت می‌کنید و این موضوع نگرانی‌های آن‌ها در مورد ریسک‌های اطلاعاتی را کاهش می‌دهد.

این کتاب برای چه کسانی مفید است؟

رشد داده‌ها بی‌سابقه است و هنگامی که این رشد با افزایش قوانین و مقررات و جریمه‌ها همراه باشد، سازمان‌ها ناچارند به برنامه‌های حکمرانی داده‌های خود نظر کنند تا مطمئن شوند که به متهم بعدی اهمال کاری تبدیل نمی‌شوند. بنابراین، هر سازمان باید درک صحیحی از داده‌هایی که جمع‌آوری می‌کند، مسئولیت و مقررات مرتبط با آنها، و این که چه کسی به آنها دسترسی دارد، ایجاد کند. اگر می‌خواهید بدانید که در این مسیر چه چیزی لازم است، از چه خطراتی باید آگاه باشید و چه ملاحظات باید در ذهن داشته باشید، این کتاب برای شما است.

این کتاب برای هر کسی می‌خواهد با پیاده‌سازی ابزارها و فرایندها، داده‌ها را قابل اعتماد کند مناسب است. در این کتاب می‌بینید که چگونه افراد، فرایندها و فناوری با هم کار می‌کنند تا امکان انطباق ممیزی شده و تدوین سیاست‌های داده‌ای مورد وثوق سازمان را ایجاد نمایند.

منافع حاصل از حکمرانی داده، چندوجهی است. از مباحث حقوقی و انطباق با قوانین و مقررات گرفته تا بهبود مدیریت ریسک و توانایی ایجاد درآمد بالا و صرفه‌جویی در هزینه‌ها با ایجاد محصولات و سرویس‌های جدید. با خواندن این کتاب می‌آموزید که چگونه کنترل و بینش روی دارایی‌های داده ایجاد کرده و به تبع آن میان هم‌تایان خود مزیت رقابتی خلق کنید.

قراردادهای استفاده شده در کتاب

قلم مورب^۱

نشان‌دهنده نام‌های جدید، آدرس‌های وب، ایمیل و نام و پسوند فایل‌ها است.

این تصویر نشان‌دهنده نکته یا پیشنهاد است.



این تصویر نشان‌دهنده یادداشتی عمومی است.



این تصویر نشان‌دهنده هشدار یا احتیاط است.

