INSO
15816-1
1st.Edition
2019
Identical with
ISO/IEC 38505-1: 2017

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۵۸۱۶-۱
چاپ اول
۱۳۹۸

دارای محتوای رنگی

فناوری اطلاعات- حکمرانی فناوری اطلاعات- حکمرانی داده‌ها

قسمت ۱:

کاربرد استاندارد ISO/IEC 38500 درحکمرانی داده‌ها

Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data

ICS: 35.020

استاندارد ملی ایران شمارهٔ ۱-۱۵۸۱۶ (چاپ اول):سال ۱۳۹۸

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج - شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.gov.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.2592 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.gov.ir

Website: http://www.isiri.gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط ۴ کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن تـوجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات-حکمرانی فناوری اطلاعات- حکمرانی داده‌ها- قسمت ۱: کاربرد استاندارد ISO/IEC 38500 درحکمرانی داده‌ها»

رئیس:	**سمت و/یا محل اشتغال:**
رضوی، ناصر (دکتری رباتیک و هوش مصنوعی)	عضو هیات علمی- دانشگاه تبریز
دبیر:	
تفسیری، حامد (کارشناسی مهندسی کامپیوتر، نرم افزار)	رئیس اداره فناوری اطلاعات و ارتباطات - اداره کل استاندارد آذربایجان شرقی
اعضا:(اسامی به ترتیب حروف الفبا)	
آزادی مطلق، مهدی (دکتری رمزنگاری)	کارشناس ارشد پژوهش و توسعه- شرکت مدیریت امن الکترونیکی کاشف
اطهری‌فرد، علیرضا (کارشناسی ارشد مدیریت فناوری اطلاعات)	مدیر واحد طرح و برنامه -شرکت مدیریت امن الکترونیکی کاشف
اکبری سروری، شبنم (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	عضو مستقل
بدرزاده، فریبا (کارشناسی مهندسی کامپیوتر، شبکه)	کارشناس- اداره کل استاندارد آذربایجان شرقی
جلالی، امیرحسین (کارشناسی ارشد مهندسی کامپیوتر، نرم‌افزار)	عضو هیات علمی- دانشگاه آزاد اسلامی واحد تبریز
جمشیدی، حامد (کارشناسی ارشد مهندسی کامپیوتر، نرم‌افزار)	رئیس اداره فناوری اطلاعات و ارتباطات - اداره کل ارتباطات و فناوری اطلاعات آذربایجان شرقی
خاکپور، علی (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	کارشناس- شرکت دیتا سیستم
رحمانی خوشه‌مهر، علی (کارشناسی ارشد مهندسی کامپیوتر، نرم‌افزار)	رئیس اداره فناوری اطلاعات و ارتباطات- شرکت شهرک‌های صنعتی آذربایجان شرقی
شکری قراجه، زهرا (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	کارشناس- شرکت نبوغ تجارت آسیا

اعضا: (اسامی به ترتیب حروف الفبا)	**سمت و/یا محل اشتغال:**
صادقی، محسن (کارشناسی ارشد فرهنگ و زبان‌های باستانی ایران (خط‌شناسی)	کارشناس مستندسازی و استانداردهای امنیت اطلاعات- شرکت مدیریت امن الکترونیکی کاشف
صالحی، اصغر (کارشناسی ارشد مدیریت صنعتی)	کارشناس- سازمان ملی استاندارد ایران
کوشنده، علی (کارشناسی ارشد معماری)	کارشناس- شرکت پگاسوس
فایند، یونس (کارشناسی ارشد مهندسی کامپیوتر، هوش مصنوعی)	رئیس اداره فناوری اطلاعات و ارتباطات - شرکت مخابرات آذربایجان شرقی
فروغی فر، مسعود (کارشناسی ارشد مهندسی کامپیوتر، نرم‌افزار)	کارشناس- اداره کل ارتباطات و فناوری اطلاعات آذربایجان شرقی
مطلب‌زاده، رقیه (دکتری مهندسی مکانیک)	عضو هیات علمی- دانشگاه آزاد اسلامی واحد تبریز
معروف، سینا (کارشناسی مهندسی کامپیوتر، سخت‌افزار)	کارشناس استاندارد
میکائیلی، هادی (کارشناسی ارشد مهندسی کامپیوتر، نرم‌افزار)	عضو هیات علمی- دانشگاه آزاد اسلامی واحد شبستر
ناظری، نیما (کارشناسی مهندسی کامپیوتر، نرم‌افزار)	عضو مستقل

ویراستار:	
معروف، سینا (کارشناسی مهندسی کامپیوتر، سخت‌افزار)	کارشناس استاندارد

فهرست مندرجات

عنوان **صفحه**

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- حکمرانی فناوری اطلاعات- حکمرانی داده‌ها- قسمت ۱: کاربرد استاندارد ISO/IEC 38500 در حکمرانی داده‌ها» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تهیه و تدوین شده است، در ششصد و سی و چهارمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۸/۰۳/۲۱ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی است و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 38505-1: 2017, Information technology- — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data

مقدمه

هدف این استاندارد، ارائه اصول، تعاریف و مدلی برای بدنهٔ حاکمیت است که در ارزشیابی، هدایت و پایش پردازش و استفاده داده‌ها در سازمان‌هایشان استفاده می‌شود.

این استاندارد، استاندارد مشاوره‌ایِ سطح بالا و اصول‌گرا است. علاوه بر ارائه راهنمایی‌های گسترده دربارهٔ نقش بدنهٔ حاکمیت، سازمان‌ها را تشویق می‌کند تا از استانداردهای مناسب برای حصول اطمینان از حاکمیت داده‌ها استفاده کنند.

همه سازمان‌ها از داده استفاده می‌کنند و بخش عمده‌ای از این داده‌ها به صورت الکترونیکی در سیستم‌های فناوری اطلاعات (IT)[1] ذخیره می‌شود. با پیدایش محاسبات ابری، تحقق پتانسیل «اینترنت چیزها»[2] و استفاده روزافزون از روش‌های تحلیلی «کلان داده‌ها»[3]، داده‌ها برای تولید، جمع‌آوری، ذخیره و استخراج اطلاعات مفید آسان‌تر می‌شوند. این سیل داده‌ها با توجه به الزامات و مسئولیت‌های ضروری برای بدنهٔ حاکمیت، اطمینان می‌دهد که فرصت‌های ارزشمند قدرت نفوذ دارند و داده‌های حساس محافظت شده و ایمن هستند.

این استاندارد، برای ارائه راهنمایی‌هایی به اعضای بدنهٔ حاکمیت به‌منظور اعمال رویکرد اصول‌گرا برای حاکمیت داده فراهم شده است تا ارزش داده‌ها را همراه با کاهش ریسک‌های مربوط به این داده‌ها، افزایش دهد. استاندارد ISO/IEC 38500 اصول و مدلی را برای بدنهٔ حاکمیت سازمان‌ها برای راهنمایی استفادهٔ فعلی آن‌ها و طرح‌ریزی برای استفاده آینده از فناوری اطلاعات (IT) ارائه می‌کند و استانداردی است که در اینجا اعمال می‌شود.

این استاندارد همانند استاندارد ISO/IEC 38500، در ابتدا به بدنهٔ حاکمیت یک سازمان می‌پردازد و به همان اندازه بدون توجه به اندازه سازمان یا صنعت یا بخشی از آن، اعمال خواهد شد. حاکمیت متمایز از مدیریت است و بنابراین ما با ارزیابی، هدایت و پایش استفاده از داده‌ها، به جای ماشینی کردن ذخیره، بازیابی یا مدیریت داده‌ها سروکار داریم. گفته می‌شود که درک برخی از فنون و مدیریت داده‌ها به منظور بیان راهبردها و خط‌مشی‌های احتمالی که می‌تواند توسط بدنهٔ حاکمیت، هدایت شود، مشخص می‌شود.

1 -Information Technology
2 - Internet of things
3 - Big data

فناوری اطلاعات- حکمرانی فناوری اطلاعات- حکمرانی داده‌ها- قسمت ۱: کاربرد استاندارد ISO/IEC 38500 در حکمرانی داده‌ها

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، ارائه اصول راهنما برای اعضای بدنهٔ حاکمیت سازمان‌ها (شامل صاحبان، مدیران، شرکا، مدیران اجرایی یا مشابه آن‌ها) برای استفاده اثربخش، کارا و قابل‌قبول داده‌ها در سازمان‌هایشان با روش‌های زیر است:[۱]

- اعمال اصول حاکمیت و مدل ISO/IEC 38500 برای حاکمیت داده‌ها،
- دادن اطمینان به ذی‌نفعان که در صورت پیروی از اصول و شیوه‌های پیشنهاد شده توسط این استاندارد، آن‌ها می‌توانند به حاکمیت داده‌ها سازمان اعتماد داشته باشند،
- اطلاع‌رسانی و ارائه راهنمایی به بدنهٔ حاکمیت در استفاده و حفاظت داده‌ها در سازمان‌های خود و
- ایجاد واژگان برای حاکمیت داده‌ها.

این استاندارد، همچنین می‌تواند راهنمایی‌هایی برای یک جامعه وسیع‌تر شامل موارد زیر ارائه دهد:

- مدیران اجرایی،
- کسب‌وکارهای خارجی یا متخصصان فنی، مانند متخصصان حقوقی یا حسابداری، انجمن‌های خُرد یا صنعتی یا بدنه‌های حرفه‌ای،
- ارائه‌دهندگان خدمت داخلی و خارجی (شامل مشاوران) و
- ممیزان.

در حالی که این استاندارد به حاکمیت داده‌ها و استفاده از آن در یک سازمان می‌پردازد، به طور کلی در استاندارد ISO/IEC/TC 38501، راهنمایی‌هایی دربارهٔ مقدمات پیاده‌سازی برای حاکمیت مؤثر فناوری اطلاعات یافت می‌شود. ساختار استاندارد ISO/IEC/TC 38501 می‌تواند به شناسایی عوامل داخلی و خارجی مربوط به حاکمیت IT و تعریف نتایج سودمند و شناسایی شواهد موفقیت کمک کند.

این استاندارد، برای حاکمیت استفاده کنونی و آتی داده‌هایی که توسط سیستم‌های فناوری اطلاعات ایجاد، جمع‌آوری، ذخیره یا واپایش می‌شوند و بر فرآیندهای مدیریتی و تصمیمات مربوط به داده‌ها تأثیر دارند، کاربرد دارد.

---

[۱]

این استاندارد، حاکمیت داده‌ها را به عنوان زیرمجموعه یا حوزه‌ای از حاکمیت فناوری اطلاعات تعریف می‌کند به‌طوری‌که خود آن زیرمجموعه یا حوزه‌ای از حاکمیت سازمان و در مورد شرکت‌ها، حاکمیت شرکتی می‌باشد.

این استاندارد برای همه سازمان‌ها، شامل شرکت‌های دولتی و خصوصی، هستارهای[1] دولتی و سازمان‌های غیرانتفاعی و نیز برای همه سازمان‌ها با هر اندازه‌ای از کوچک‌ترین تا بزرگ‌ترین، صرف‌نظر از میزان وابستگی آن‌ها به داده‌ها، کاربرد دارد.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مرجع زیر برای کاربرد این استاندارد الزامی است:

2-1 ISO/IEC 38500, Information technology — Governance of IT for the organization

یادآوری- استاندارد ملی ایران شماره ۱۲۰۴۷: سال ۱۳۹۵، فناوری اطلاعات -حاکمیت فناوری اطلاعات (IT) برای سازمان، با استفاده از استاندارد ISO/IEC 38500 :2008 تدوین شده است.

۳ اصطلاحات و تعاریف

در این استاندارد، علاوه بر اصطلاحات و تعاریف ارائه شده در استاندارد ISO/IEC 38500، اصطلاحات و تعاریف زیر نیز به‌کار می‌رود.[2]

۳-۱

گمنام‌سازی[3]

anonymization

---

1 - Entities

۲ - اصطلاحات و تعاریف به‌کار رفته در استانداردهای ISO و IEC در وبگاه‌های www.electropedia.or و www.iso.org/ob قابل‌دسترس است.

فرآیندی که در آن اطلاعات شناسایی‌پذیر شخصی (PII) به گونه‌ای برگشت‌ناپذیر، طوری تغییر می‌کند که بخش مهمی در PII دیگر نتواند مستقیم یا غیرمستقیم و به‌وسیله واپایش‌کنندهٔ PII به تنهایی یا با همکاری بخش دیگر شناسایی شود.

[منبع: زیربند ۲-۲ استاندارد ملی ایران شماره ۱۷۶۴۳: سال ۱۳۹۲]

۲-۳

کلان داده

big data

مجموعه (های) داده‌هایی با مشخصه‌هایی، مانند: حجم، سرعت، تنوع، تغییرپذیری، صحت و غیره که برای دامنه مشکل خاصی در نقطه معینی در زمان نمی‌تواند با استفاده از فناوری‌ها و فنون کنونی/ موجود/ ایجادشده/ رایج به منظور استخراج ارزش، به‌طور مؤثری پردازش شود.

یادآوری ۱- اصطلاح کلان‌داده‌ها معمولاً به روش‌های مختلفی استفاده می‌شوند، برای مثال به عنوان فناوری مقیاس‌پذیر مورد استفاده برای ساماندهی کلان داده‌های مجموعه داده‌های وسیع.

[منبع: زیربند 3.2.1 استاندارد ISO/IEC 20546]

۳-۳

رایانش ابری

cloud computing

الگویی برای توانمندسازی دسترسی شبکه‌ای به خزانه سنجش‌پذیر و انعطاف‌پذیری از منابع تسهیم‌شدنی فیزیکی یا مجازی با فراهم‌آوری و راهبری امکان خودیاوری به درخواست است.

یادآوری- مثال‌هایی از منابع عبارتند از: کارسازها[1]، سیستم عامل‌ها، شبکه‌ها، نرم‌افزار، برنامه‌های کاربردی و تجهیزات ذخیره‌سازی.

[منبع: زیربند 3.2.5 استاندارد ISO/IEC 17788: 2014]

۴-۳

تعهدپذیری داده‌ها

data accountability

تعهدپذیری داده‌ها و کاربرد آن‌هاست.

یادآوری- «کاربرد» داده‌ها شامل همه فعالیت‌های مرتبط با داده‌ها است.

1 -servers

۵-۳

ناشناس‌سازی

de-identification

اصطلاح عمومی برای هرگونه فرآیند برداشتن وابستگی میان مجموعه داده‌های شناسایی‌کننده و موضوع داده است.

[منبع: زیربند 3.18 استاندارد ISO/TS 25237:2008]

۶-۳

اینترنت چیزها

internet of things
IoT

زیرساخت جهانیِ جامعه اطلاعاتی که ارائه خدمات پیشرفته را با اتصال (فیزیکی و مجازی) چیزها بر پایهٔ فناوری‌های اطلاعاتی و ارتباطی موجود، هم‌کنش‌پذیر[1] و تکامل‌یافته امکان می‌بخشد.

یادآوری ۱- اینترنت چیزها با بهره‌جویی کامل از شناسایی، داده‌گیری، پردازش و توانمندی‌های ارتباطاتی، خدماتی را به همه گونه برنامه کاربردی ارائه می‌دهد و همزمان، از این که الزامات مربوط به حریم خصوصی و امنیت برآورده شده است، اطمینان پیدا می‌کند.

یادآوری ۲- در چشم‌اندازی گسترده، اینترنت چیزها را می‌توان نگرشی با بیان و کاربرد فناورانه و اجتماعی دانست.

[منبع: Rec. ITU-T Y.2060]

۷-۳

یادگیری ماشینی

machine learning

فرآیندی است که از الگوریتم‌ها به جای کدنویسی رویه‌ای[2] استفاده می‌کند تا امکان یادگیری از داده‌های موجود را برای پیش‌بینی پیامدهای آینده فراهم سازد.

۸-۳

نام‌مستعارسازی

Pseudonymization

فرآیند به‌کار گرفته شده برای اطلاعات شناسایی‌پذیر شخصی (PII) که اطلاعات شناسایی‌کننده را با نام مستعار جایگزین می‌کند.

---

1 -Interoperable
2 - Procedural coding

یادآوری ۱- نام‌مستعارسازی می‌تواند به‌وسیله مدیران و راهبرانِ PII یا به‌وسیله واپایش‌کننده‌های PII انجام شود. مدیران و راهبران PII می‌توانند با استفاده از «نام‌مستعارسازی»، پیوسته از منبع یا خدمتی بهره ببرند؛ بی آنکه هویت خود را نزد آن منبع یا خدمت (یا میان چند خدمت گوناگون) آشکار سازند و در عین حال، چیزی هم از پاسخگویی یا تعهدپذیری‌شان کاسته نشود.

یادآوری ۲- در نام‌مستعارسازی، این احتمال که (مجموعه محدودی) از ذی‌نفعان حریم خصوصی - به غیر از واپایش‌کنندهٔ PII داده نام‌مستعاریافته - هستند که توان شناختنِ هویت مدیران یا راهبران PII را – بر پایهٔ نام‌های مستعار ایشان و داده‌های پیوند یافته به ایشان – شناسایی کنند، منتفی نیست.

[منبع: زیربند ۲-۲۴ استاندارد ملی ایران شماره ۱۷۶۴۳: سال ۱۳۹۲، کلمه اشخاص به شخصی تغییر یافته است]

۳-۹

اطلاعات شخصی قابل‌شناسایی
کارکرد PII

personally identifiable information
PII function

هر اطلاعاتی که: الف- می‌تواند برای شناسایی راهبر PII که اطلاعات از این دست به ایشان ربط پیدا می‌کند، یا ب- مستقیم یا غیرمستقیم به مدیر و راهبر PII ربط دارد یا می‌تواند ربط داشته باشد.

یادآوری- برای تعیین این که آیا راهبر PII قابل‌شناسایی است یا خیر؟ باید همه ابزارهایی را که ذی‌نفع حریم خصوصیِ دارنده آن داده‌ها یا هر گروه دیگری می‌تواند به‌طور منطقی برای شناسایی فرد واقعی به کار گیرد، در شمار آورد.

[منبع: زیربند ۲-۹ استاندارد ملی ایران شماره ۱۷۶۴۳: سال ۱۳۹۲]

۳-۱۰

راهبر PII

PII principal

فرد واقعی که اطلاعات شخصی قابل شناسایی (PII) به او مرتبط است.

یادآوری- بسته به صلاحیت قضایی، حفاظت از داده‌های خاص و قانون‌گذاری حریم خصوصی واژه مترادف «نماد داده‌ها» نیز می‌تواند به جای عبارت «راهبر PII» استفاده شود.

[منبع: زیربند ۲-۹ استاندارد ملی ایران شماره ۱۷۶۴۳: سال ۱۳۹۲]

۴ حاکمیت خوبِ داده

۴-۱ فواید حاکمیت خوبِ داده

حاکمیت خوبِ داده به بدنهٔ حاکمیت برای دستیابی به اطمینان از این که کاربرد داده‌ها در سازمان، به گونه‌ای مثبت است و از راه‌های زیر به عملکرد آن سازمان یاری می‌رساند، کمک می‌کند:

- نوآوری در خدمات، بازارها و کسب‌وکار؛
- پیاده‌سازی و به‌کارگیری مناسبِ دارایی‌های داده‌ای؛
- شفافیت در مسئولیت‌پذیری و پاسخگویی و تعهّدپذیری برای حفاظت و توانایی بالقوه برای افزودن ارزش؛
- رساندن پیامدهای زیانبار و نسنجیده به کمترین میزان.

سازمان‌های برخوردار از حاکمیت خوبِ داده باید چنین باشند:

- سازمان‌هایی چنان اعتمادپذیر که صاحبان و کاربران داده با آنها دادوستد کنند؛
- توانِ ارائه داده‌های اعتمادپذیر برای تسهیم را داشته باشند؛
- نگاهبان داشته‌های فکری و دیگر ارزش‌های برآمده از داده باشند؛
- سازمان‌هایی برخوردار از خط‌مشی و شیوهٔ تاراندن رخنه‌گران و پیشگیری از کارهای کلاهبرداران؛
- آمادهٔ کمینه‌سازی تاثیر نقض داده‌ها باشند؛
- از زمان و چگونگی بازاستفاده از داده‌ها آگاه باشند؛
- توانایی نشان دادن شیوه‌های سازمان‌دهی داده‌های خوب را دارا باشند.

این استاندارد، اصولی را برای استفاده مؤثر، کارآمد و قابل‌قبول داده‌ها ایجاد می‌کند. به بدنهٔ حاکمیت، با اطمینان از این که سازمان‌هایشان از این اصول پیروی می‌کنند، در مدیریت ریسک‌ها و تشویق بهره‌برداری از فرصت‌های ناشی از سامان‌دهی ایمن و تفسیر دقیق داده‌های کیفی کمک خواهد شد.

حاکمیت خوبِ داده به بدنهٔ حاکمیت در حصول اطمینان از انطباق با الزامات (نظارتی، قانونی، قراردادی) در استفاده قابل‌قبول و سامان‌دهی داده‌ها کمک می‌کند.

این استاندارد، مدلی برای حاکمیت داده‌ها ایجاد می‌کند. مخاطرهٔ پیش رویِ بدنهٔ حاکمیت که به وظایف خود عمل نمی‌کند، با توجه به مدل استفاده مناسبِ اصول، کاهش می‌یابد.

تمهیدات ناکافی برای حاکمیت داده می‌تواند سازمان را در معرض چندین ریسک از جمله موارد زیر قرار دهد:

- جریمه‌های عدم مطابقت با قوانین، مخصوصاً قوانین مربوط به معیارهای حریم خصوصی مورد نیاز؛
- از دست دادن محرمانگی داده‌های کسب‌وکار، برای نمونه: دستورکارها یا ویژگی‌های طراحی؛
- کاهش اعتماد ذی‌نفعان، شرکای کسب‌وکار، مشتریان و عموم مردم؛
- ناتوانایی در انجام کارکردهای حیاتی سازمانی به دلیل نبود اطمینان یا داده‌های مرتبط با کسب‌وکار؛
- افزایش رقابت از طریق استفاده راهبردی داده‌ها توسط رقبا.

بدنهٔ حاکمیت در موارد زیر می‌توانند پاسخگو و تعهدپذیر باشند:

- نقض حریم خصوصی، هرزنامه، سلامتی و ایمنی، حفظ سوابق قوانین و مقررات؛

- عدم مطابقت استانداردهای اجباری مرتبط با امنیت، مسئولیت اجتماعی؛
- مسائل مربوط به حقوق مالکیت معنوی.

۴-۲ مسئولیت‌های بدنه حاکمیت

اعضای بدنهٔ حاکمیت در قبال حاکمیت داده مسئولیت‌پذیر و برای استفاده اثربخش، کارا و قابل‌قبول از داده‌ها توسط سازمان متعهد هستند.

اختیار، مسئولیت‌پذیری و پاسخگویی و تعهدپذیری بدنهٔ حاکمیت برای استفادهٔ موثر، کارا و قابل‌قبول داده‌ها، از مسئولیت‌پذیری کلی حاکمیت سازمان و تعهدات آن به ذی‌نفعان خارجی از جمله تنظیم‌کننده‌های مقررات ناشی می‌شود.

تمرکز کلیدی نقش بدنهٔ حاکمیت در حاکمیت داده این است که اطمینان دهد سازمان ارزش را از سرمایه‌گذاری در داده‌ها و فناوری اطلاعات مرتبط به دست می‌آورد. در حالی که ریسک را مدیریت می‌کند و به محدودیت‌ها توجه دارد.

علاوه بر این، بدنهٔ حاکمیت باید اطمینان دهد که درک روشنی از داده‌هایی که توسط سازمان و هدفی که برای آن مورد استفاده قرار می‌گیرد وجود دارد و سیستم مدیریتی مؤثری برای اطمینان از برآورده شدن تعهدات مانند حفاظت داده‌ها، حریم خصوصی و احترام به دارایی فکر و اندیشه وجود دارد.

۴-۳ بدنه حاکمیت و سازوکارهای نظارتی

بدنهٔ حاکمیت باید سازوکارهای نظارتی را برای حاکمیت داده‌هایی که با سطح کسب‌وکار وابسته به داده مناسب هستند، ایجاد کند.

بدنهٔ حاکمیت باید درک روشنی از اهمیت داده‌ها در راهبردهای کسب‌وکار سازمان و همچنین ریسک راهبردی بالقوه سازمان برای استفاده داده‌ها را داشته باشد. میزان توجه یک بدنهٔ حاکمیت به داده‌ها باید مبتنی بر این عوامل باشد.

بدنهٔ حاکمیت باید اطمینان حاصل کند که اعضای آن و سازوکارهای حاکمیتی مربوط (مانند ممیزی، مدیریت ریسک و کمیته‌های مربوط) و همچنین مدیران، دانش و درک لازم از اهمیت داده‌ها را دارند.

بدنهٔ حاکمیت ممکن است کمیته‌ای فرعی را ایجاد کند تا به کمک آن بر استفادهٔ سازمان از داده‌ها با دیدگاه راهبردی نظارت کند. نیاز به کمیته فرعی به اهمیت داده‌های سازمان و اندازه آن بستگی دارد.

بدنهٔ حاکمیت باید اطمینان دهد که چارچوب حاکمیت خوبی برای حاکمیت و مدیریت داده‌ها ایجاد شده است.

بدنهٔ حاکمیت باید اثربخشی سازوکارها برای حاکمیت و مدیریت داده‌ها را با الزام کردن فرآیندهایی مانند ممیزی و ارزیابی‌های مستقل پایش کند تا اطمینان حاصل کند که حاکمیت مؤثر است.

۵ اصول، مدل و جنبه‌های حاکمیت خوبِ داده

همان‌گونه که در استاندارد ISO/IEC 38500 مشخص شده است، حاکمیت فناوری اطلاعات، زیرمجموعه یا دامنه حاکمیت سازمانی، یا دربارهٔ شرکت، حاکمیت شرکتی است. این استاندارد، بر پایه استاندارد ISO/IEC 38500 برای بررسی خاص داده‌ها و استفاده از آن‌ها توسط سازمان تدوین شده است.

استاندارد ISO/IEC 38500 شش اصل را برای حاکمیت خوب فناوری اطلاعات به شرح زیر مشخص می‌کند:

الف- مسئولیت‌پذیری؛

ب- راهبرد؛

پ- اکتساب؛

ت- عملکرد،

ث- انطباق؛

ج- رفتار انسانی.

استاندارد ISO/IEC 38500 همچنین مدلی را برای حاکمیت فناوری اطلاعات معرفی می‌کند که چرخه «ارزیابی- هدایت- پایش» (EDM)[1] را ایجاد می‌کند. مدل «ارزیابی- هدایت- پایش» سه وظیفه اصلی حاکمیت فناوری اطلاعات را توصیف می‌کند و این نکته را یادآوری می‌کند که «مرجع مجازشناس جنبه‌های خاص فناوری اطلاعات می‌تواند به مدیران درون سازمان تفویض شود. با وجود این، پاسخگویی و تعهّدپذیری برای استفادهٔ موثر، کارا و قابل‌قبول فناوری اطلاعات توسط سازمان در بدنهٔ حاکمیت باقی می‌ماند و نمی‌تواند تفویض شود.»

نواحی وسیع پاسخگویی و تعهّدپذیری مربوط به داده‌ها، همراه با جریان داده‌ها و فرآیند «دریچه‌بندی»[2] که در آن راهبرد و خط‌مشی‌ها برای حمایت از پاسخگویی و تعهّدپذیری هستند، در بند ۶ نشان داده شده است.

برای به‌کارگیری اصول و مدل در حاکمیت داده، ضروری است که جنبه‌های خاص داده‌ای حاکمیت برای راهنمایی بررسی شود. این جنبه‌ها به تمام داده‌ها اعمال می‌شود و باید در درک داده‌ها و تأثیر آن‌ها در سرتاسر سازمان در نظر گرفته شود. آن‌ها همچنین فرصت‌هایی را که استفادهٔ داده‌ها (مخصوصاً با فناوری‌های در حال پیدایش) برای سازمان فراهم می‌کنند و نیز پاسخگویی و تعهّدپذیری‌های اضافی را که داده‌ها در اختیار بدنهٔ حاکمیت قرار می‌دهند، مشخص می‌کنند.

جنبه‌های خاص داده‌های حاکمیتی که در این استاندارد معرفی شده است، عبارت‌اند از:

1 - Evaluate-Direct-Monitor
2 -Gatng

- **ارزش:** داده، مادهٔ خام برای دانشِ مفید است. بعضی از داده‌ها، ممکن است خیلی مفید نباشند، در حالی که داده‌های دیگر برای سازمان بسیار ارزشمند هستند. با وجود این، ارزش تا زمانی که توسط سازمان استفاده نشود، شناخته شده نیست و بنابراین همه داده‌ها برای بدنهٔ حاکمیت که در نهایت در قبال آن‌ها پاسخگو و تعهّدپذیر است، جالب توجه است. اصطلاح «ارزش» در این مورد شامل کیفیت و کمیت داده‌ها، بهنگام بودن[1] آن‌ها، متن (که خودش «داده» به شمار می‌آید) و هزینه ذخیره‌سازی، نگهداری، کاربری و وارهایی (دورریزی)[2] آن‌ها نیز می‌شود.
- **ریسک:** طبقات مختلف داده‌ها، سطوح مختلف ریسک را به وجود می‌آورند و بدنهٔ حاکمیت باید ریسک‌های داده‌ها و نحوه هدایت مدیران برای مدیریت این ریسک‌ها را درک کند. ریسک‌ها نه تنها در نقض داده‌ها، بلکه در سودجویی از داده‌ها و نیز ریسک‌های رقابتیِ وارد شده در استفاده نادرست داده‌ها آشکار می‌شوند.
- **تنگناها:** بیشتر داده‌ها با تنگناهای استفاده از آن‌ها همراه هستند. بعضی از این موارد، از طریق قوانین، مقررات یا تعهدات قراردادی از خارج بر سازمان تحمیل می‌شوند و شامل مسائلی مانند حریم خصوصی، حق نشر، منافع تجاری و غیره است. تنگناهای دیگر داده‌ها شامل تعهدات اخلاقی یا اجتماعی یا خط‌مشی‌های سازمانی است که استفاده از داده‌ها را محدود می‌کند. لازم است در تنگنای استفاده از داده‌ها توسط سازمان، به راهبردها و خط‌مشی‌ها توجه شود.

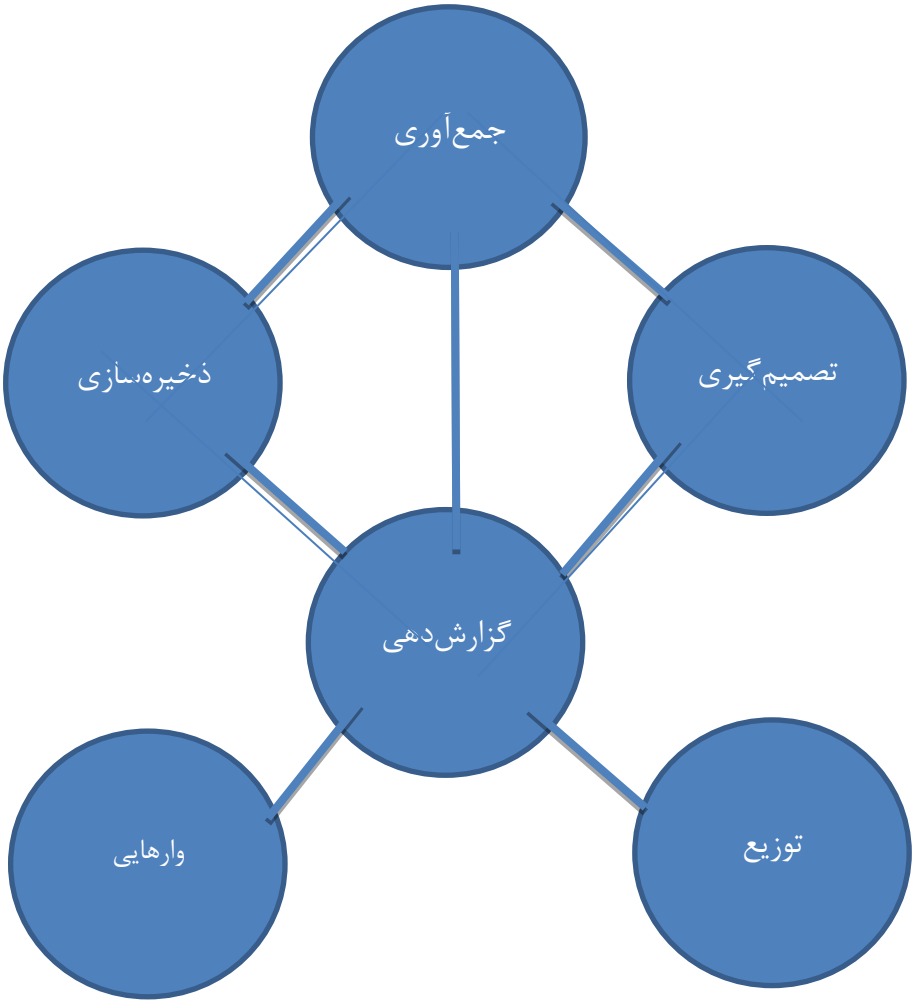
داده‌ها و استفاده از آن‌ها توسط سازمان‌ها به طور فزاینده‌ای برای همه سازمان‌ها و ذی‌نفعان حائز اهمیت است. با به‌کارگیری اصول، مدل و جنبه‌های خاص داده‌ای حاکمیت مندرج در این استاندارد، بدنهٔ حاکمیت باید بتوانند فعالیت‌هایی را انجام دهند که سرمایه‌گذاری خود را در استفاده از داده‌ها بیشینه کنند، ریسک‌های مورد بحث را مدیریت کنند و حاکمیت خوبی برای سازمان‌هایشان فراهم کنند.

۶ تعهدپذیری داده‌ها

۶-۱ کلیات

داده‌ها دارایی کلیدی هر سازمان است. داده‌ها برای ردگیری کسب‌وکار (مانند مردم، حسابداری، موجودی و غیره) و به عنوان ماده خام دانش، نوآوری و بینش استفاده می‌شود. پاسخگویی و تعهّدپذیری داده‌ها و استفاده از آن‌ها بر عهده بدنه حاکمیت سازمان می‌ماند.

1 - Timeliness
2 - Dispose



یادآوری- مانند هر مدل، این نمودار به منظور نشان دادن مفاهیم خاص مربوط به اقلام مورد توجه بدنه حاکمیت ساده شده است. عناوین عناصر ارائه شده نشان‌دهندهٔ فعالیت است و توضیحات بیشتر در زیر نوشته شده است.

شکل ۱- نقشه پاسخگویی و تعهّدپذیری داده

شکل ۱، مناطق تعهدپذیری داده‌ها را در یک سازمان نشان می‌دهد. توضیحات بیشتر عناصر نقشه در زیر نوشته شده است.

نقشه، موضوعاتی را که از دیدگاه حاکمیت برای هر سازمان و برای هر نوع کسب‌وکاری جالب توجه هستند، شناسایی می‌کند. در حالی که فرآیندهای واقعی و پیاده‌سازی‌ها، جزء مسئولیت‌های مدیریت هستند، خطوط نشان می‌دهد که جریان داده‌ها و سازوکار دریچه‌بندی هر جا که ضروری باشد برای اطمینان از خط‌مشی‌ها و راهبردهای حاکمیت وضع و تعهدپذیری برآورده می‌شوند. جنبه‌های خاص داده‌های حاکمیت در زمینه این پاسخگویی و تعهّدپذیری‌ها در بند ۹ بیشتر بحث شده‌اند.

این استاندارد بر حاکمیت داده متمرکز است که نباید با مدیریت داده‌ها اشتباه گرفته شود. در حالی که بدنه حاکمیت با به‌کارگیری اصول حاکمیت مشخص شده در بند ۷ سروکار دارد، حوزه مدیریت داده‌ها روش‌های تعریف‌شده‌ای برای پردازش داده‌ها و نیز سازوکارهایی برای اطمینان از محرمانگی، یکپارچگی و بازیافت داده‌ها دارد. مثالی از چرخه عمر مدیریت داده‌ها در شکل ۲ نشان داده شده است.

شکل ۲- مثال چرخه عمر مدیریت داده‌ها

۶-۲ جمع‌آوری

فعالیت جمع‌آوری شامل فرآیندهای اکتساب، گردآوری و پردازش، یادگیری از تصمیم‌گیری‌های قبلی و مفاهیم استخراج شده بیشتر از مجموعه داده‌های دیگر (داخلی یا خارجی) است.

داده‌ها به شکل‌های زیادی موجود هستند و می‌توانند برای استفادهٔ سازمان به روش‌های مختلفی شامل روش‌های زیر، ایجاد و جمع‌آوری شوند:

- **ورود داده‌ها:** ورود داده‌ها با استفاده از برنامه‌های کاربردی که یا در درون سازمان (برای مثال، در یک سیستم برنامه‌ریزی منابع سازمانی (ERP)[1] یا برنامه کاربردی رایانامه) یا به شکل خارجی از طریق وب‌سایت، برنامه کاربردی تلفن همراه یا برنامه کاربردی مشابه به دست می‌آید.
- **تراکنش‌ها از سامانه‌های دیگر:** ورود یا به‌روزرسانی داده در سیستم‌های دیگر می‌تواند از طریق تبادل داده‌های الکترونیکی (EDI)[2] یا دیگر فرآیندهای واسطه‌سازی[3] جریان یابد.
- **حسگرها:** مقدار زیادی از داده‌ها از طریق سیستم‌های دستگاهی مانند حسگرها به سازمان می‌رسد. حسگرها طیف وسیعی از افزاره‌های اکتساب داده‌ها شامل رویدادنگارهای وب‌سایت[4]، منابع رسانه‌های اجتماعی و افزاره‌های «اینترنت چیزها» هستند که دربرگیرنده افزاره‌های روزمره از حسگرهای دمایی ساده تا تلویزیون‌ها، خودروها، چراغ‌های راهنمایی و ساختمان‌ها هستند. داده‌های حاصل از حسگرها همچنین می‌توانند شامل سیگنال‌های بالقوه ضروری مانند اعلام خطر و هشدارها باشند.
- **زمینه (متن) جدید:** می‌توان داده‌های حاصل از گزارش‌ها را با داده‌های دیگر ترکیب کرد تا اطلاعات بیشتری فراهم شود که بازخورد آن به داده‌های سازمان برمی‌گردد. در بسیاری موارد، این داده‌های بیشتر، زمینه جدیدی به داده‌های اصلی می‌دهند و ممکن است نیاز باشد متفاوت از داده‌های اصلی با آن‌ها

1 - Enterprise Resource Planning
2 - Electronic Data Interchange
3 - Interfacing
4 - Web site logs

برخورد شود. داده‌های متنی جدید می‌توانند از تصمیماتی که ممکن است بـه داده‌هـای موجـود مـرتبط باشد یا ارزش بدهد، حاصل شود.

- **عضویت:** داده‌ها ممکن است از طریق عضویت داده‌ها یا ذخیره داده‌های مجازی برای سازمان در دسترس باشند.

۶-۳ ذخیره

فعالیت ذخیره شامل قرار دادن داده‌ها در جایی است که به لحاظ فیزیکی یا منطقی بتوان بازیابی کـرد. ایـن فعالیت، داده‌های ذخیره‌شده روی افزاره‌هایی که خود سازمان به‌کار می‌گیرد، افزاره‌هـای خـارج از سـازمان و مخزن‌های مجازی مانند خوراک[1] داده‌هایی که فقط در صورت نیاز تلفیق می‌شوند را دربرمی‌گیرد. در هر یک از موارد، می‌توان داده‌های ذخیره‌شده را برای گزارش کردن مقاصد و کاربری‌هـایی کـه بـه «تصـمیم‌گیـری دربارهٔ وارهایی» می‌انجامند، نگهداری کرد.

همان‌گونه که داده‌ها از طریق اقدامات فوق جمع‌آوری می‌شوند، به محل ذخیرهٔ داده‌ها کـه ایمـن هسـتند و مدیریت و احتمالاً بایگانی می‌شوند وارد می‌شوند. مقدار داده‌هایی که سازمان‌ها واپایش می‌کننـد، بـه دلیـل فناوری‌های جدید مانند اینترنت چیزها که برای جمع‌آوری داده‌ها از حسگرها استفاده می‌کنند و همچنین به خاطر ابر داده‌ها که از مقدار زیادی داده‌ها برای جستجوی روند و پیش‌بینی با استفاده از یـادگیری ماشـینی استفاده می‌کنند، به سرعت رو به افزایش است. بسیاری از این فناوری‌های نوپدید در زیست‌بوم‌های «رایانش ابری عمومی» اجرا می‌شوند که که در آن زیست‌بوم‌ها، کاستن از هزینه‌های قابلیت‌های پردازش و ذخیره در مقیاس بزرگ امکان‌پذیر شده، با هزینه‌های بسیار پایین انجام می‌شوند.

گاهی سازمان، داده‌ها را در جایی بیرون از خود ذخیره می‌کند و معمولاً چنین کاری را با «عملیات میزبـانی بیرون از مکان» -برون‌سپاری کار ذخیرهٔ داده‌ها- انجام می‌دهد. رایانش ابری این کـار را بـه مرحلـه دیگـری می‌برد؛ مرحله‌ای که در آن، سازمان کارخواه (مشتری) نمی‌تواند عملیات ذخیره‌سازی را ببیند. علاوه بر این، سازمان ممکن است از «مخزن مجازی»[2] استفاده کند که داده‌ها بـه عنـوان خـوراک داده ارائـه مـی‌شـوند و می‌توانند به طور مستقیم در گزارش‌ها یا تحلیل‌ها جریان یابند.

همچنین باید یادآوری شود که اگرچه سازمان ممکن است داده‌ها را در این محلِ ذخیره واپـایش کنـد ولـی ممکن است به دلیل حقوق مالکیت معنوی مانند حق نشر یا دیگر مسائل قانونی از جمله: قوانین مربـوط بـه سامان‌دهی اطلاعات شخصی یا سلامتی مالکیّت داده‌ها با سازمان نباشد. مراقبت‌هـای خاصـی ممکـن اسـت برای ذخیره و استفاده داده‌ها بین مرزهای حوزه قضایی لازم باشد. در هر صورت، نظارت بر داده‌ها بـه عهـده بدنهٔ حاکمیت است.

---

۱ - نوعی قالب داده‌ای برای عرضهٔ محتواهایی به کاربران که پیاپی روزآمد می‌شوند.

2 - Virtual store

۶-۴ گزارش

فعالیت گزارش شامل استخراج و تحلیل دستی یا خودکار داده‌ها برای حمایت از تصمیم‌گیری، توزیع یا وارهایی است.

قابلیت مهم سیستم اطلاعات، استخراج داده‌ها از مخزن داده‌ها به صورت خوراک داده‌ها است. این خوراک باید دارای خواص مرتبطی مانند کیفیت و رایج بودن داده‌ها باشد تا کسب‌وکار بتواند سودمندی آن را برای گزارش‌هایی که از داده‌ها تهیه می‌شوند، تعیین کند.

طی مدت فرآیند استخراج و گزارش‌دهی، ممکن است از خوراک‌های داده‌های بسیاری استفاده شود که می‌توانند از مخزن داده‌های درون سازمان یا از مخزن داده‌های مجازی بیرون سازمان حاصل شوند. ترکیبی از این خوراک‌های داده‌ها ممکن است زمینه جدیدی برای داده‌ها ایجاد کند. این زمینه جدید به نوبت خود داده‌های جدیدی بوده و باید در جایی که فرآیند جمع‌آوریِ عادی روی می‌دهد، بازخوردی از فرآیند ایجاد و جمع‌آوری داده‌ها باشد.

برنامه‌های کاربردی همچنین می‌توانند گزارش‌ها را تهیه و نیز داده‌های موجود را به‌روزرسانی کنند و این داده‌های جدید، دوباره از فرآیند ایجاد پیروی می‌کنند.

دیگر فنون استخراج و تحلیل مانند داده‌کاوی و یادگیری ماشینی را می‌توان برای به دست آوردن بینش بیشتر، پیش‌بینی نتایج آتی و تصمیم‌گیری خودکار به‌کار برد. دوباره این داده‌های جدید ایجاد و جمع‌آوری می‌شوند.

می‌توان از گزارش‌ها برای پالایش[1] داده‌ها با هدف افزایش سودمندی‌شان، یا ایجاد امکان توزیع و وارهاییشان بهره بُرد. برای مثال، داده‌های حاصل از حسگرها را می‌توان برای پیدا کردن روندها و همزمان حذف اطلاعات شناسایی‌پذیر شخصی به روش‌هایی مانند: گمنام‌سازی و نام‌مستعارسازی گرد آورده، جمع کرد و به روش‌هایی همسان و مشابه داده‌های اصلی را هم به دست آورد و هم دور ریخت.

۶-۵ تصمیم

فعالیت تصمیم زمانی روی می‌دهد که تصمیم‌گیری بر اساس بررسی گزارش انجام شود. تصمیم‌گیری‌ها توسط افراد درون سازمان یا به روش‌های خودکار انجام می‌شود.

دلیل اصلی برای داشتن داده‌ها، تصمیم‌گیری است و ارزش داده‌ها به این است که چگونه تصمیمات اتخاذ شده را بهبود بخشید. گزارش‌ها (شامل گزارش‌دهی روی صفحه نمایش) بررسی می‌شوند تا اطلاعات برای اتخاذ تصمیم فراهم شود.

---

1 -Filter

بدنهٔ حاکمیت از طریق یک فرآیند تفویض اطمینان می‌یابد که تصمیمات اتخاذ شده برای سطح مسئولیت این تصمیمات، مناسب هستند. زمانی که تصمیم‌گیری خودکار از طریق فرآیندهای ساده جریان داده‌ها یا الگوریتم‌های پیچیده‌تر یادگیری ماشینی انجام می‌شود، این موضوع از اهمیت خاصی برخوردار است. در هر صورت، بدنهٔ حاکمیت دربارهٔ تمام تصمیمات پاسخگو و تعهدپذیر بوده و باید اطمینان یابد که آن‌ها واپایش‌های مناسبی دارند و اگر لازم باشد، مداخله‌های انسانی برای مقابله با هرگونه تعصبات، تبعیض با نمایه‌سازی در فرآیند تصمیم‌گیری اعمال می‌شود.

از آنجا که فرآیند تصمیم‌گیری به داده‌ها ارزش می‌دهد، بازخورد اطلاعات («سودمندی» داده‌ها) می‌تواند به فرآیندهای جمع‌آوری و ایجاد داده‌ها بازگردد. با ایجاد این نگهداری داده و حلقه بازخورد، می‌توان گزارش‌های ایجاد شده، خوراک دادهٔ مورد استفاده و در نهایت، داده‌ای که خوراک سیستم است، را به خوبی تنظیم کرد. این حلقه همچنین ارزش تصمیم‌ها را افزایش می‌دهد و به نوبه خود می‌تواند کسب‌وکار را بهبود بخشد.

۶-۶ توزیع

فعالیت توزیع شامل استخراج یا رونوشت داده‌ها از طریق فعالیت گزارش‌دهی برای انتقال به طرف‌های خارجی است.

داده‌ها را می‌توان از مخزن داده استخراج کرد و به خارج از سازمان توزیع کرد. این کار به دلایلی مانند موارد زیر روی می‌دهد:

- گزارش‌دهی به خارج، برای مثال به یک مرجع مجازشناس حاکمیتی ضروری است؛
- این داده‌ها بخشی از تبادل داده کسب‌وکار به کسب‌وکار (B2B)[1]، استفاده مشتری یا فعالیت مشابه است؛
- داده‌ها برای مثال به یک آژانس تبلیغاتی یا شرکت تحقیقاتی فروخته می‌شود؛
- داده‌ها قسمتی از کسب‌وکار انتشارات سازمان است، برای مثال داده‌های کسب‌وکار (به عبارت دیگر، داده‌ها محصول هستند)؛
- توزیع مجاز نشده است، در این صورت این امر به عنوان نقض داده‌ها طبقه‌بندی می‌شود.

۶-۷ وارهایی

فعالیت وارهایی معمولاً شامل: شناسایی داده‌های دورریز از طریق انجام فعالیت گزارش‌دهی و سپس پاک کردن آن داده‌ها و همهٔ رونوشت‌هایشان از «انبار (مخزن) داده» برای همیشه و نیز اگر داده‌ای به مصرف رسیده باشد، قطع ارتباط آن داده با محل مصرفش است.

1 - business-to-business

پیچیدگی روزافزون تحلیل داده‌ها، ابزار داده‌کاوی و یادگیری، ارزش داده‌های موجود را افزایش می‌دهد، زیرا اطلاعات بیشتری را می‌توان از داده‌های بیشتر استخراج کرد. این حقیقت و همچنین هزینه کاهش‌یافتهٔ نگهداری داده‌ها، نیاز به وارهایی داده‌ها را کاهش می‌دهد.

اما هنوز دلایلی برای برداشت مقداری داده از مخزن داده، از طریق فعالیت گزارش‌دهی و وارهایی ایمن آن داده‌ها وجود دارد.

- برای کاهش ریسک نشت داده. اگر داده‌ها وجود نداشته باشند دیگر نمی‌توان آن را به نادرستی توزیع کرده، به کار گرفت.
- برای حذف داده‌های نامناسب یا نادرست. اگرچه ممکن است از داده‌های قدیمی‌تر برای تحلیل روند استفاده شود، اما ممکن است دیگر مرتبط و درست نباشند.
- برای اعمال حق به فراموشی سپردن. ممکن است مشتریان بخواهند داده‌هایشان حذف شوند.
- برای انطباق با موافقت‌نامه‌های قراردادی با مشتریان یا تأمین‌کنندگان.
- برای انطباق با الزامات یا مقررات قانونی.

به همین ترتیب ممکن است دلایلی مانند: مقررات مربوط به بهداشت یا قوانینی که نگهداری داده را الزام می‌کنند وجود داشته باشند.

۷ راهنمای حاکمیت داده‌ها- اصول

۷-۱ کلیات

استاندارد ISO/IEC 38500، شش اصل برای حاکمیت خوب فناوری اطلاعات ارائه می‌دهد. زیربندهای زیر، راهنمایی برای چگونگی استفاده از این اصول برای حاکمیت داده ارائه می‌دهد.

شیوه‌های توصیف شده جامع و فراگیر نیستند، اما نقطه شروعی برای بحث دربارهٔ مسئولیت‌های بدنهٔ حاکمیت برای حاکمیت داده فراهم می‌کنند؛ یعنی شیوه‌های توصیف شده راهنمای پیشنهادی هستند.

مسئولیت هر سازمانی، به‌طور جداگانه، شناسایی اقدامات خاص لازم برای پیاده‌سازی اصول، توجه به ماهیت سازمان و به‌کارگیری تحلیل مناسب جنبه‌های خاص داده‌ها است که در بند ۹ به آن اشاره شده است.

۷-۲ اصل ۱- مسئولیت

بدنهٔ حاکمیت دربارهٔ مسئولیت‌های مربوط به استفادهٔ سازمان از داده‌ها پاسخگو است و باید اطمینان حاصل کند که درون سازمان، مسئولیت‌های خود را درک کرده و پذیرفته است.

این مسئولیت‌ها عبارت‌اند از:

- گسترش در سراسر سازمان و فراتر از عملکرد یا بخش فناوری اطلاعات، یا فعالیت‌های بنیادین فناوری اطلاعات؛
- شامل داده‌های کلیدی مربوط به فعالیت‌های کسب‌وکار مانند بازاریابی که داده‌ها برای اطلاع‌رسانی طرح‌های محصول و توسعه محصول استفاده شده‌اند و نیز برای راهنمایی طراحی و ساخت محصولات جدید جمع‌آوری می‌شوند؛
- شامل وضعیت‌هایی که خودِ داده، محصول یا خدمتی است که سازمان ارائه می‌دهد. چنین وضعیت‌هایی شامل محتوایی مانند موسیقی یا فیلم‌ها و اطلاعاتی مانند گزارش‌های آب‌وهوا یا بازار سهام است؛
- پوشش کل چرخه‌عمر داده‌ها.

۷-۳ اصل ۲- راهبرد

بدنهٔ حاکمیت دربارهٔ راهبرد داده‌ها که با راهبرد کلی سازمان هم‌راستاست، از جمله قابلیت‌های کنونی و بعدی، پاسخگو است. این راهبرد باید:

- شامل طرح‌هایی برای استفاده از داده‌هایی باشد که اهداف راهبردی کلی کنونی و بعدی را نشان می‌دهد؛
- مجاز به پیشرفت‌های فناوری و انتظارات بازار باشد؛
- همه قسمت‌های نقشه پاسخگویی و تعهّدپذیری داده‌ها را پوشش دهد؛
- به جنبه‌های خاص داده‌های حاکمیتی (ارزش، ریسک، محدودیت‌ها) توجه کند؛
- انتظاراتی را که ممکن است نیاز به بازنگری راهبرد کلی برای پاسخگویی و تعهّدپذیری فرصت‌ها یا ریسک‌های جدید داشته باشد، تنظیم کند.

۷-۴ اصل ۳- دریافت (اکتساب)

بدنهٔ حاکمیت دربارهٔ اکتساب داده‌ها (با جمع‌آوری یا خرید، یا به عنوان محصول جانبی فعالیت کسب‌وکار) پاسخگو است و باید اطمینان یابد که چنین اکتساب‌هایی با در نظر گرفتن موارد زیر مناسب هستند:

- اکتساب با استفادهٔ موردنظر و/یا بیان شدهٔ آن درون سازمان و نیز استفادهٔ خارجی، در صورت توزیع داده‌ها، سازگار است.
- ارزیابی ارزش، ریسک‌ها و محدودیت‌های مربوط به کاربرد پیشنهادی و مدیریت مجموعه داده‌های به دست آمده یا جریان‌های داده‌ها با راهبرد داده‌ها هم‌راستا است.

۷-۵ اصل ۴- عملکرد

بدنهٔ حاکمیت باید معیارهای عملکرد مربوط را شناسایی کند و اطمینان یابد که اگر نیاز باشد، به آن معیارها توجه کافی می‌شود و اقدام‌های اصلاحی نیز اعمال می‌شوند.

معیارهای عملکردی باید شامل موارد زیر باشند:

- کاربری خوب و به سزای داده‌ها تا چه اندازه مؤیّد و پشتیبان تصمیم‌گیری‌هایِ سازمان است؛
- کاربری خوب و به سزای داده‌هایی که با تأمین‌کنندگان یا مشتریان به اشتراک نهاده شده‌اند، تا چه اندازه مؤیّد و پشتیبان تصمیم‌گیری‌ها است؛
- نرخ پذیرش مجموعه داده‌های جدید و داده‌های در گردش (جاری) درون سازمان؛
- سودِ سرمایه‌گذاری روی داده‌ها، شامل داده‌هایی که توزیع شده‌اند؛
- بهایی که سازمان به «ارزش کلّی داده‌ها» می‌دهد در قیاس با بهایی که سازمان‌های رقیب یا مشابه به «ارزش کلّی داده‌ها» می‌دهند.

۷-۶ اصل ۵- همخوانی

بدنهٔ حاکمیت باید اطمینان یابد که سازمان تعهدات خارجی را می‌داند و پیروی می‌کند و به درستی تعریف می‌کند، پیاده می‌کند و از انطباق با خط‌مشی‌های داخلی مناسب اطمینان می‌یابد. چنین تعهدات و خط‌مشی‌هایی باید شامل موارد زیر باشد:

- تمامی مجموعه داده‌ها و جریان‌های داده‌ها مطابق با خط‌مشی‌های امنیتی که نیازها و تعهدات سازمان را برآورده می‌کند، ایمن شود؛
- ساماندهی صحیح PII؛
- پیاده‌سازی مناسب خط‌مشی و شیوه حفظ داده‌ها در سراسر سازمان؛
- درک تمام تعهدات قانونی مربوط به داده‌ها و حصول اطمینان از این که تعهدات در سراسر سازمان برآورده شده‌اند.

۷-۷ اصل ۶- رفتار انسانی

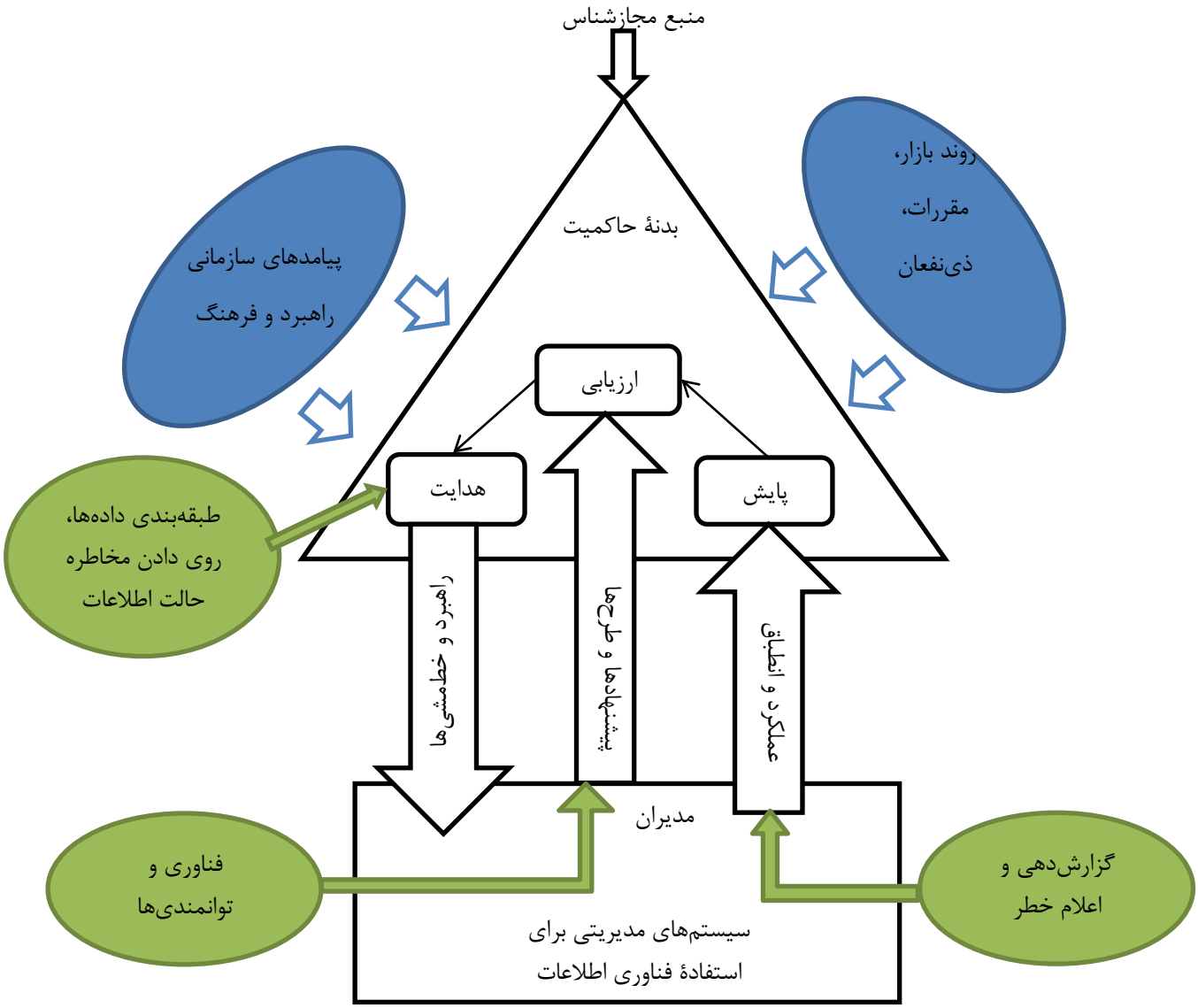
بدنهٔ حاکمیت در برابر کاربری داده‌ها در سراسر سازمان متعهّد و پاسخگوست، آن چنان که رفتارهای انسانی شناسایی شده، به درستی در نظر گرفته شده باشند. چنین ارج‌گذاری‌ای به رفتار انسانی باید موارد زیر را در برگیرد:

- خط‌مشیی برای هدایت کاربری پذیرفتهٔ داده‌ها و افزاره‌ها در سراسر سازمان؛
- فرهنگ سازمانیِ در پیوند با داده‌ها باید مشوّقِ اشتراک‌گذاری، حفظ و تفسیر مناسبِ داده‌ها باشد؛

- تأثیر و الزامات رفتار انسانی ذی‌نفعان.

۸ راهنمای برای حاکمیت داده‌ها- مدل

۸-۱ به‌کارگیری مدل



شکل ۳- حاکمیت مدل فناوری اطلاعات- برنامه کاربردی برای حاکمیت داده

بدنهٔ حاکمیت باید داده‌ها را از طریق سه وظیفه اصلی زیر نظارت و مدیریت کنند:

الف- ارزیابی استفاده کنونی و بعدی از داده‌ها؛

ب- آماده‌سازی مستقیم و پیاده‌سازی راهبردها و خط‌مشی‌ها برای اطمینان‌یابی از برآورده شدن اهداف کسب‌وکار با کاربرد داده‌ها؛

پ- پایش انطباق با خط‌مشی‌ها و عملکرد در برابر راهبردها.

مجازشناسی جنبه‌های خاص داده‌ها ممکن است به مدیران درون سازمانی تفویض شود. با وجود این، پاسخگویی و تعهّدپذیری برای استفاده موثر، کارا و قابل‌قبول داده‌ها توسط سازمان، همچنان با بدنهٔ حاکمیت است و نمی‌تواند تفویض شود.

شکل ۳، فشارهای خاص وارد بر بدنهٔ حاکمیت را در رابطه با داده‌ها و استفاده از آن‌ها توسط سازمان نشان می‌دهد. ذی‌نفعان، از جمله: مشتریان، کارکنان و تنظیم‌کنندگان مقررات همگی در این حوزه ذی‌نفع هستند. این شکل، همچنین انواع دروندادهای[1] مورد نیاز چرخه EDM را که به داده‌ها مربوطند، نشان می‌دهد. نواحی‌ای که در آن، درونداد مدیریت می‌تواند در فعالیت‌های هدایت، ارزیابی و پایش به بدنهٔ حاکمیت کمک کند، در نمودار نشان داده شده‌اند.

۸-۲ الزامات داخلی

بدنهٔ حاکمیت، راهبرد کلی را برای کسب‌وکار ایجاد می‌کند. با وجود این، استفاده از داده‌ها در همه صنایع و حاکمیت، بسیار حائز اهمیت است؛ به این معنی که باید بدنهٔ حاکمیت برای برآوردن تعهدات خود به ذی‌نفعان، استفاده از داده‌ها را به عنوان بخشی از راهبرد کلی بررسی کند.

لازم است بدنهٔ حاکمیت، استفادهٔ بالقوه از داده‌ها را توسط خود سازمان یا رقبای خود بررسی کند و راهبرد را برای پشتیبانی از پیامدهای مطلوب جهت‌دهی کند. این عمل ممکن است شامل خرید و فروش داده‌ها باشد.

کسب‌وکار، مرزهای فرهنگی در زمینهٔ کاربرد داده‌ها توسط سازمان دارد. بدنهٔ حاکمیت باید فرهنگ داده‌ای را به گونه‌ای ترسیم کند تا اطمینان یابد که آن فرهنگ با راهبرد داده‌های مورد نیاز برای رسیدن به اهداف کلی بدنهٔ حاکمیت هم‌راستاست. از آنجایی که داده با تصمیمات گرفته شده با آن ارزش پیدا می‌کند، این فرهنگ داده‌ای می‌تواند منجر به رفتارهای سازمانی شود که مربوط به دسترسی داده‌ها، شیوه‌های سامان‌دهی خوب داده‌ها و فرآیندهای تصمیم‌گیری در همه سطوحی است که متکی به گزارش‌هایی در زمینه مرتبط هستند.

۸-۳ فشارهای خارجی

سازمان ممکن است برای اطمینان از سازگاری با فشارهای نیروهای بازاری که در آن فعالیت می‌کند، نیاز به تنظیم راهبردها و خط‌مشی‌های خود داشته باشد. چنین نیروهایی عبارت‌اند از:

- انتظارات مشتری با در نظر گرفتن وارهایی، کیفیت و تعامل با داده‌های موجود و

1 -inputs

- رقبایی که از داده‌ها برای بهبود یا گسترش محصولات، خدمات یا فرآیندهای خود استفاده می‌کنند.

قوانین و مقررات و همچنین الزامات ذی‌نفعان ممکن است بین بازارها متفاوت باشند و بدنهٔ حاکمیت نیاز دارد اطمینان یابد که راهبردها و خط‌مشی‌هایی برای استفاده کنونی و بعدی داده‌ها می‌تواند به طور گسترده‌ای در این بازارها اعمال شود. چنین تنگناها و تعهداتی ممکن است در فعالیت‌های مختلف پاسخگویی و تعهّدپذیری داده‌ها اعمال شود، از جمله:

- داده‌ها را چگونه می‌توان گرد آورد تا شامل آگاه‌سازی حریم خصوصی و الزامات رضایت دربارهٔ جمع‌آوری و استفاده از اطلاعات شخصی باشند،
- الزامات نگهداری و وارهایی داده‌ها،
- تعهدات تصمیم‌گیری برای برخورد مناسب با تعصبات، تبعیض و نمایه‌سازی و

مسائل مربوط به مالکیت معنوی دربارهٔ به اشتراک‌گذاری یا بازاستفاده از داده‌ها.

۸-۴ ارزیابی

در ارزیابی حاکمیت داده برای سازمان، بدنهٔ حاکمیت باید به الزامات داخلی و فشارهای خارجی وارد بر سازمان توجه کند.

علاوه بر این، بدنهٔ حاکمیت باید استفاده کنونی و بعدی داده‌ها را بررسی و داوری کند که شامل موارد زیر است:

- استفاده داخلی از داده‌ها و فناوری‌ها و فرآیندهای مرتبط،
- استفاده از داده‌ها توسط رقبا، سازمان‌های دیگر، دولت‌ها و افراد،
- ارزیابی مجموعه در حال تحول قوانین، مقررات، انتظارات اجتماعی و
- عوامل دیگری که استفاده از داده‌ها را واپایش می‌کند و بر آن تأثیر می‌گذارد.

فناوری‌های مدیریت داده‌ها به سرعت در حال تغییر است و بدنهٔ حاکمیت باید پیشنهادهای مدیران را برای توضیح این فناوری‌ها و تأثیر بالقوه آن‌ها بر سازمان درخواست کند. چنین فناوری‌هایی می‌توانند تأثیر قابل توجهی بر تمام جنبه‌های داده‌ها شامل هزینه، بینش و حریم خصوصی داشته باشند. در بسیاری از موارد، این اثرات می‌تواند فراتر از مدیریت داده‌ها باشد و فرصت‌های کسب‌وکار جدید و به‌طور بالقوه ریسک بزرگ‌تری برای سازمان فراهم آورند. بدون اعمال خود این فرصت‌ها، بدنهٔ حاکمیت می‌تواند سازمان را در معرض ریسک رو به افزایش ناشی از رقبا، تغییر انتظارات بازار و مسائل رو به افزایش مربوط به انطباق قرار دهد.

بدنهٔ حاکمیت همچنین باید از توانمندی‌های مدیریت داده‌های سازمان مطلع باشد. برای مثال:

- سازمان تا چه اندازه‌ای می‌تواند نقض داده را بهبود دهد؛

- اطلاعات صحیح چگونه به آسانی می‌تواند در قالب درست برای کمک به تصمیم‌گیری در همه سطوح تحویل داده شود؛
- آیا سازمان، فناوری‌های جدید، مانند: رایانش ابری را برای افزایش توانمندی‌های خود به‌کار می‌گیرد.

راهبردها و خط‌مشی‌های حاکمیت داده فقط در صورتی می‌تواند پیاده‌سازی شود که سازمان منابع لازم و توانایی لازم را برای پیاده‌سازی چنین خط‌مشی‌هایی داشته باشد.

۸-۵ هدایت

بدنهٔ حاکمیت باید مسئولیت‌پذیری برای آماده‌سازی و پیاده‌سازی مستقیم راهبردها و خط‌مشی‌ها را اختصاص دهند.

راهبردها و خط‌مشی‌های استفاده کنونی و بعدی داده‌ها برای سازمان باید در جهت اهداف زیر باشد:

- **بیشینه کردن ارزش سرمایه‌گذاری سازمان در داده‌ها**: داده‌ها مانند هر دارایی دیگر در سازمان، نیاز به سرمایه‌گذاری دارد. این درست است که داده‌های خارج از سازمان جمع‌آوری شده، در شخص سوم ذخیره یا به عنوان یک خدمت استفاده می‌شود و مانند هر سرمایه‌گذاری دیگر، سازمان می‌خواهد اطمینان یابد که بازدهی خوبی از داده‌ها حاصل می‌شود. ارزش نهایی داده‌ها این است که چگونه استفاده از آن، تصمیم‌گیری را بهبود می‌بخشد، اما ممکن است سازمانی بتواند داده‌ها را برای استفاده به دیگران بفروشد.
- **مدیریت ریسک مرتبط با داده‌ها با توجه به ریسک‌پذیری آن‌ها:** برخی داده‌ها مانند بررسی محصول یا بلندپروازی برای بازار سهام ناشناخته، ارزش کسب‌وکار بالایی دارد و لازم است برای به‌کارگیری و حفاظت داده‌ها از منابع مناسبی استفاده شود. ارزش و ریسک مربوط به مدیریت این داده‌ها بیشتر از انواع دیگر داده‌ها است و راهبردها و خط‌مشی‌ها باید پذیرش طرح رده‌بندی داده‌ها را منعکس کنند.
- **اطمینان از سطح صحیح مباشرت[1] داده‌ها:** بدنهٔ حاکمیت دربارهٔ داده‌ها و استفاده آن‌ها، از جمله تصمیماتی که برای داده‌ها گرفته می‌شود، پاسخگو است؛ بنابراین، فعالیت‌های پاسخگویی و تعهّدپذیری داده‌ها باید به طرز مناسبی درون سازمان تفویض شود.

این عناصر همگی به «نگرش اطلاعات» سازمان و اثربخشی آن در به‌کارگیری داده‌ها برای اهداف کسب‌وکار سازمان کمک می‌کند. این کار، فرهنگ داده‌ای یک سازمان، راهبرد کلی آن، ریسک‌پذیری آن، سطوح امنیتی درک شده آن، میزان کار مبتنی بر دانش و معیارها و ارزش آن بر داده‌ها و استفاده از آن را نشان می‌دهد.

1 - Stewardship

۸-۶ پایش

بدنهٔ حاکمیت باید از طریق سیستم‌های اندازه‌گیری مناسب، عملکرد استفاده از داده‌های سازمان را پایش کنند. آن‌ها باید بتوانند به خودشان اطمینان دهند که راهبردهای مربوط به داده‌ها به درستی پیاده‌سازی می‌شوند و استفاده و مدیریت داده‌ها با خط‌مشی‌های داخلی و الزامات خارجی مانند مقررات و الزامات نظارت بر داده‌ها مطابقت دارد.

استفاده از ابزار گزارش‌دهی و تحلیل در تصمیم‌گیری باید برای درک ارزش داده‌ها و بهبود فرآیند تصمیم‌گیری اندازه‌گیری باشد.

نواحی دیگر که نظارت بدنهٔ حاکمیت به دلیل راهبردی یا مقررات ممکن است از اهمیت زیادی برخوردار باشد، عبارت‌اند از:

- استفاده از PII شامل نگرانی‌های مربوط به حفظ حریم خصوصی، الزامات رضایت و شفافیت استفاده از داده‌هاست (به استاندارد ISO/IEC 29100 مراجعه شود)؛
- استفاده از سیستم مدیریت موثر امنیت اطلاعات، همان‌گونه که در استاندارد ISO/IEC 27001 توصیف شده است، اهمیت راهبردی داده‌ها را نشان می‌دهد. این کار باید شامل خوراک داده‌های شخص سوم و مدیریت داده‌ها در خدمات رایانش ابری باشد، برای مثال: استاندارد ISO/IEC 27017. این استاندارد، راهنمایی برای واپایش‌های امنیتی اطلاعات را در برخی موارد فراهم می‌کند. چنین واپایش‌هایی کافی نخواهند بود و بدنهٔ حاکمیت نیاز دارد تا به اعتماد و درستی‌سنجی تکیه کند؛
- الزامات نگهداری و وارهایی داده‌ها؛
- بازاستفاده، به اشتراک‌گذاری یا فروش داده‌ها و حقوق مربوط به آن، صدور مجوز یا حق نشر؛
- اصول حسابرسی مناسب برای هنجارهای فرهنگی، تعصب، تبعیض یا نمایه‌سازی در تصمیم‌گیری.

۹ راهنمای حاکمیت داده- جنبه‌های خاص داده

۹-۱ کلیات

در بسیاری از سازمان‌ها، حجم داده‌ها هنگام استفاده به صورت نمایی افزایش می‌یابد. این عمل نتیجه تغییرات اخیر در فناوری است که از لحاظ اقتصادی آن را برای پردازش مجموعه کلان-داده‌ها مناسب می‌سازد.

این قابلیت به این معنی است که استفاده از داده‌ها برای بسیاری از سازمان‌ها، بدون در نظر گرفتن صنعت، هسته کسب‌وکار است.

زمانی که داده‌ها در سازمانی استفاده می‌شوند -خواه در خارج از سازمان ذخیره شود، توسط دیگران نشر یابد، خواه در «مالکیت» مشتری باشد- با ارائه تصمیم‌گیری بهتر یا اطلاعات افزون‌تر، امکان ایجاد ارزش

جدید در سازمان را فراهم می‌آورند. همچنین تعدادی از پاسخگویی‌ها و تعهّدپذیری‌ها بر سازمان تحمیل می‌شوند.

داده‌ها دارایی غیرمصرفی با بسیاری از ویژگی‌ها و جنبه‌های مرتبط هستند و مستلزم آن است که توسط بدنهٔ حاکمیت سازمان به عنوان اقلامی که ممکن است تأثیر راهبردی قابل توجهی در کل سازمان داشته باشند، در نظر گرفته شوند.

۹-۲ ارزش

۹-۲-۱ کلیات

داده‌ها می‌تواند به عنوان یک ماده خام برای اطلاعات مفید توزیع شوند و به فروش روند. فروشی که در آن از طریق اشتراک، خوراک داده‌ای همچون نشریه یا وب‌سایت، ارزش پولی به داده‌ها اختصاص می‌دهد.

ارزش کسب‌وکار در داده‌ها، اندازه‌گیری چگونگی بهبود تصمیماتی است که از اطلاعات موجود در آن نشأت می‌گیرد. برای استخراج اطلاعات از داده‌ها لازم است تا داده‌ها دارای کیفیت، بهنگام بودن، متن (زمینه)، حجم و به طور بالقوه ویژگی‌های دیگری برای مطابقت با الزامات فرآیندهای تصمیم‌گیری باشند.

۹-۲-۲ کیفیت

کیفیت داده‌ها، اندازه دقیق چگونگی محفوظ‌سازی[1] واقعیت‌هایی است که برای نشان دادن آن تلاش می‌شود.

ارزشی که از داده‌ها مشتق می‌شود، به بخشی از کیفیت داده‌ها مطابق با درستی مورد نیاز فرانامه‌های[2] مختلف تصمیم‌گیری بستگی دارد.

در برخی موارد، مانند: اطلاعات مالی، مجموعه‌ای از داده‌های با کیفیت بالا، به‌روزرسانی شده و در قالب مناسب برای تصمیم‌گیرندگان، برای مثال: سرمایه‌گذاران ارائه شوند، ضروری است. با وجود این، در موارد دیگر ممکن است مجموعه‌ای از داده‌ها با کیفیت پایین‌تر به تصمیم‌گیری‌های خوب، برای مثال: دربارهٔ تحلیل روند منجر شوند.

۹-۲-۳ بهنگام بودن

داده‌ها، اطلاعاتی را برای تصمیم‌گیری بهبودیافته فراهم می‌کنند و بیشتر تصمیمات وابسته به زمان هستند، بنابراین یک خاصیت مهم داده‌ها، بهنگام بودن و رایج بودن آن‌هاست.

1 - Encapsulate
2 - Scenario

با تمام عناصر کیفیت داده‌ها، بهنگام بودن داده‌ها بستگی به تصمیم‌گیری‌ها دارد. برای مثال، تصمیم‌گیری‌های خودکار در یک سیستم ترمز ضد قفل، روی داده‌های به‌روزرسانی شده و در مدت کوتاهی تحلیل می‌شود. این مدت زمان بسیار متفاوت‌تر از زمان مورد نیاز برای تحلیل سود سالانه است.

۹-۲-۴ زمینه

به کار بردن زمینه به داده‌ها اجازه می‌دهد که اطلاعات از آن حاصل شود. این زمینه، به شکل داده‌های افزون‌تر، می‌تواند بر خط‌مشی‌های اعمال شده بر اطلاعات جدید حاصل شده تأثیر بگذارد، برای مثال: ترکیب داده‌های فروش با اطلاعات پستی ممکن است PII را نشان دهد که نیاز به سامان‌دهی متفاوت داده‌ها دارد.

متن، عامل مهمی در تصمیم‌گیری است زیرا می‌تواند هنجارهای فرهنگی و تعصب را به وجود آورد و منجر به تفسیر متفاوت داده‌ها و در نتیجه تصمیم‌گیری بالقوه متفاوتی شود.

۹-۲-۵ حجم

حجم داده‌ها می‌تواند بر ارزش آن‌ها تأثیر بگذارد. مقدار زیادی از داده‌های همخوان می‌توانند اعتماد به روند یا پیش‌بینی را افزایش دهند، اما برای رسیدن به اطمینان ممکن است فنون مختلفی نیاز باشند.

۹-۳ ریسک

۹-۳-۱ کلیات

از آنجایی که داده‌ها دارای ارزش هستند، با ریسک نیز همراه هستند. با وجود این، برخلاف دیگر دارایی‌ها، بعضی از جنبه‌های داده‌ها به این معنی است که نمایه‌های ریسک مختلفی دارند. برای مثال، سرقت داده‌ها معمولاً شامل رونوشت‌برداری غیرمجاز داده‌ها و نه انتقال آن‌هاست.

علاوه بر این، استفادهٔ داده‌هایی مانند: PII یا داده‌های مراقبت‌های بهداشتی با مسئولیت‌های اضافی همراه است و بنابراین ریسک سازمان را افزایش می‌دهد. یک راه برای کاهش این ریسک، حذف ویژگی‌های PII از طریق فنون شناسایی‌ناپذیری شرح داده شده در استاندارد ISO/IEC 20889 است.

ریسک‌پذیری کلی برای سازمان توسط بدنهٔ حاکمیت تعیین می‌شود. همان‌طور که داده‌ها به لحاظ راهبردی، عملیاتی و مالی برای سازمان مهم هستند، ریسک‌های مربوط به داده‌ها باید توسط بدنهٔ حاکمیت بررسی شوند تا اطمینان حاصل شود که سطح مناسبی از « ریسک داده» تنظیم شده است که با ریسک‌پذیری کلی هم‌راستاست.

باید ریسک داده‌هایی که در دسترس نیستند نیز برای نفع سازمان در نظر گرفته شود. زمانی که به طور منطقی مشخص شود چنین داده‌هایی در دسترس هستند، اما بر اساس آن عمل نمی‌شود، ممکن است به ضرر سازمان باشد. همچنین این عمل ممکن است به ریسک‌های عملیاتی، مانند: داده‌های ایمنی، ریسک‌های

مالی مربوط به سرمایه‌گذاری یا ریسک‌های راهبردی، مانند: مجاز بودن انواع جدید تعاملات مشتری مربوط باشد.

۹-۳-۲ مدیریت

مدیریت ریسک در زیربند ۲-۲ استاندارد ملی ایران شماره ۱۳۲۴۵: ۱۳۸۹، به عنوان «فعالیت‌های هماهنگ‌شده برای هدایت و واپایش یک سازمان با توجه به ریسک» توصیف شده است و شامل چارچوب و فرآیند ساختاریافته برای رسیدگی به ریسک است.

ریسک اصلی مربوط به داده‌ها، از دست دادن واپایش آن است؛ با وجود این، برای سازمان ریسک‌هایی نیز در سودجویی از داده‌ها در طیفی از فعالیت‌ها در نقشه پیگیری‌پذیر داده‌ها وجود دارد.

برای تغییر فرآیندهای مدیریت ریسک برای حساب ریسک داده‌ها (هر تغییری در نمایه ریسک یا ریسک‌پذیری) در زیربند 3.2 استاندارد ISO/TR 31004:2013 توصیه شده است که «سازمان باید تغییراتی را که برای چارچوب موجود برای مدیریت ریسک لازم است، قبل از برنامه‌ریزی و پیاده‌سازی آن تغییرات و پایش مداوم اثربخشی چارچوب اصلاح شده تعیین کند».

۹-۳-۳ طرح‌های کلی طبقه‌بندی داده

بدنهٔ حاکمیت باید منابعی برای به‌کارگیری و حفاظت داده‌ها، با تأکید بر ارزش بالا و ریسک بالای داده‌ها اختصاص دهد. بعضی داده‌ها، مانند: داده‌های پژوهشی ممکن است ارزش کسب‌وکار بالایی داشته باشند زیرا داده‌ها مزیت کسب‌وکار قابل توجهی دارند. برخی داده‌ها که توسط سازمان استفاده می‌شود، در اینترنت به رایگان در دسترس است.

به عنوان بخشی از یک سیستم مدیریت امنیت اطلاعات (ISMS)[1]، باید مدیران انواع مختلف داده‌ها را با طرح طبقه‌بندی داده‌ها شناسایی کنند. چنین طرحی به سازمان اجازه می‌دهد تا سطوح مختلف منابع را برای طبقه‌های مختلف داده‌ها به‌کار گیرد. در زیربند 8.2.1 استاندارد ISO/IEC 27002:2013 بیان شده است که «اطلاعات باید بر حسب الزامات قانونی، ارزش، حیاتی بودن و حساسیت به افشا یا اصلاح غیرمجاز طبقه‌بندی شود».

۹-۳-۴ امنیت

امنیت، عنصری از مدیریت ریسک است. بدنهٔ حاکمیت باید نظارت قوی بر امنیت داده‌ها در زمینه امنیت سازمان داشته باشد.

هنگام ارزیابی راهبردی و تصویب خط‌مشی‌های امنیتی داده‌ها، می‌توان به معیارهای حفاظتی زیر در میان موارد دیگر توجه کرد:

1 - Information Security Management system

- چارچوب امنیتی فناوری اطلاعات به عنوان «چارچوب برای بهبود زیرساخت حیاتی امنیت رایانه‌ای (سایبری)» از موسسه ملی و فناوری استانداردها (NIST)[1] از برنامه‌های راه‌انداز کسب‌وکار برای هدایت فعالیت‌های امنیت رایانه‌ای به عنوان بخشی از چارچوب مدیریت ریسک کلی استفاده می‌کند؛
- ISMS مانند: مجموعه استانداردهای ISO/IEC 27000 که شامل واپایش‌های امنیتی خاص است،
- جایی که PII توسط فراهم‌کنندهٔ خدمات ابری پردازش می‌شود، استاندارد ISO/IEC 27018 واپایش‌هایی را فراهم می‌کند تا از حفاظت داده‌ها اطمینان دهد.

۹-۴ تنگناها

۹-۴-۱ کلیات

داده‌های استفاده شده توسط سازمان ممکن است با تنگناهایی همراه باشد. چنین تنگناهایی ممکن است ارزش بالقوه (استفاده و توزیع) داده‌ها را محدود کند، از جمله این که چگونه می‌توان داده‌ها را با دیگر داده‌ها ترکیب یا تجمیع کرد. چنین داده‌هایی ممکن است به طبقه‌بندی متفاوتی، برای مثال: ارزش کسب‌وکار بالا، محرمانه یا PII و از اینرو به سامان‌دهی در سراسر سازمان نیاز داشته باشد.

۹-۴-۲ مقررات و قوانین

مقررات و قوانین، از جمله: قوانین متداول و قوانین قراردادی ممکن است برای دسترسی، استفاده، ذخیره یا توزیع داده‌ها اعمال شوند و باید در فرمول‌بندی راهبردها و خط‌مشی‌های داده‌ها بدان توجه کرد.

۹-۴-۳ جامعه‌نگر

از دیدگاه راهبردی، این جنبه به «قرارداد ضمنی»[2] با جامعه مربوط است. برای مثال، هدف اصلی خدمات بهداشت عمومی، می‌تواند حفظ سلامت کل جامعه و نه تنها سلامت فردی باشد. بدنهٔ حاکمیت دربارهٔ «قرارداد ضمنی» می‌تواند به روشن کردن راهبرد داده‌ها، از جمله: چگونگی استفادهٔ داده‌ها و چگونگی تصمیم‌گیری از داده‌ها کمک کند.

۹-۴-۴ خط‌مشی سازمانی

علاوه بر الزامات خارجی که دربارهٔ استفاده از داده‌ها اعمال می‌شوند، سازمان ممکن است خط‌مشی خود را روی داده‌ها برای افزایش ارزش آن‌ها، کاهش هزینه‌های مدیریت داده‌ها، کاهش ریسک‌های مربوط به داده‌ها یا برای برآوردن الزامات دیگر اعمال کند.

1 - National Institute of Standards and Technology
2 - Implied contract

۱۰ به‌کارگیریِ نقشه تعهدپذیری داده‌ها

حاکمیت داده، بدنهٔ حاکمیت را ملزم به ارزیابی، هدایت و پایش فعالیت‌های مربوط به استفاده از داده‌ها- با توجه به عوامل و تعهدات خارجی- در سراسر سازمان می‌کند.

اعمال اصول حاکمیت فناوری اطلاعات طبق استاندارد ISO/ICE 38500، چارچوب حاکمیت فناوری اطلاعات طبق استاندارد ISO/IEC/TR 38502 و پیاده‌سازی رویکرد طبق استاندارد ISO/IEC/TS 38501 بنیانی را برای توسعه خط‌مشی و رویه مربوط به داده‌ها فراهم می‌کند.

رویکردی برای اعمال اصول و مدل در حاکمیت داده، بررسی جنبه‌های خاص داده‌های حاکمیت است. این جنبه‌ها به تمام داده‌ها اعمال می‌شوند و باید در درک داده‌ها و تأثیر آن‌ها در سراسر سازمان در نظر گرفته شوند. آن‌ها همچنین فرصت‌هایی را که استفاده از داده‌ها (مخصوصاً با فناوری‌های در حال پیدایش) برای سازمان فراهم می‌کنند و همچنین پاسخگویی و تعهّدپذیری‌های افزون‌تر را که داده‌ها برای بدنهٔ حاکمیت به وجود می‌آورند، برجسته می‌کنند.

بر این اساس، هنگامی که نقشه پاسخگویی و تعهّدپذیری داده‌ها طبق بند ۶، در پیوند با جنبه‌های گوناگون داده‌ها، همچون: ارزش، ریسک و تنگناها استفاده می‌شود، راهنمایی برای یک بازبینه[1] جامع ملاحظات برای بدنهٔ حاکمیت ارائه می‌دهد تا هنگام توسعه چارچوب حاکمیت مناسب داده‌ها برای سازمان خود به آن توجه کنند. اقدامات خاص مورد نیاز برای پیاده‌سازی اصول متناسب با ماهیت سازمان و شرایط آن بسیار متفاوت خواهد بود.

بدنهٔ حاکمیت باید از جدول ۱ به عنوان راهنمایی برای ارزیابی، پایش و هدایت فعالیت‌های سازمانی برای حاکمیت داده به‌طور کلی و برای رده‌های خاص داده‌ها - اگر مناسب باشد- استفاده کند. برای هر فعالیت پاسخگویی و تعهّدپذیری داده‌ها، باید جنبه‌های خاص داده‌ها را بررسی کرد تا نشان دهد که اقدامات لازم با توجه به سطوح بالاتر واپایش و خط‌مشی سختگیرانه‌تر برای جمع‌آوری داده‌های با ارزشِ بیشتر یا حساسیت بیشتر نیاز خواهد بود.

ارزش، ریسک‌ها و تنگناهای مربوط به مجموعه داده‌های خاص در گذر زمان، در بسامدی وابسته به عوامل بسیار از جمله اندازه سازمان، بخش و صلاحیت متفاوت خواهد بود. این مسئولیت‌پذیری بدنهٔ حاکمیت برای تعیین چرخه بازنگری مناسب برای سازمان خود است.

این بازبینه، راهنمای ایجاد چهارچوب حاکمیت را برای بدنهٔ حاکمیت فراهم می‌کند که از به‌کارگیری بیشینه ارزش داده‌ها در ریسک‌پذیری داده‌هایشان و با توجه به محدودیت‌های داخلی و خارجی پشتیبانی می‌کند.

بازبینهٔ فراهم‌شده، فراگیر نیست و بدنهٔ حاکمیت باید موقعیت خود را ارزیابی کند و لازم ببیند، اقدامات افزون‌تری انجام دهد.

---

1 -checklist

جدول ۱- نواحی داده‌ها و جنبه‌های خاص داده‌های حاکمیت

	ارزش	ریسک	تنگناها
جمع‌آوری	[ارزش ۱] بدنهٔ حاکمیت باید درباره درجه‌ای که سازمان برای دستیابی به اهداف راهبردی خود، داده‌ها را به‌کار می‌گیرد یا از آن‌ها کسب درآمد می‌کند، تصمیم‌گیری کند.	[ریسک ۱] بدنهٔ حاکمیت باید ریسک‌های مربوط به جمع‌آوری و استفاده از داده‌ها را شناسایی کند و در سطح پذیرفتنی ریسک داده‌ها در ریسک‌پذیری کلی سازمان توافق کند. این کار شامل بررسی ریسک‌های داده‌های جمع‌آوری نشده و استفاده نشده است.	[تنگنای ۱] بدنهٔ حاکمیت باید خط‌مشی‌های جمع‌آوری داده‌ها را با توجه به تنگناهایی، مانند: کیفیت، حریم خصوصی، الزامات رضایت و شفافیت استفاده تصویب کند.
ذخیره	[ارزش ۲] بدنهٔ حاکمیت باید خط‌مشی‌هایی را تصویب کند که منابع مناسبی برای ذخیره‌سازی داده‌ها و اشتراک داده‌ها تخصیص می‌دهد تا بتوان ارزش بالقوه داده‌ها را استخراج کرد.	[ریسک ۲] بدنهٔ حاکمیت باید مدیران را هدایت کند تا اطمینان یابد که یک ISMS با منابع، واپایش‌ها و اعتماد کافی در حال گسترش به فراهم‌کنندگان داده‌ها و فناوری است که از سطح ریسک‌پذیر فراتر نمی‌رود.	[تنگنای ۲] بدنهٔ حاکمیت باید مدیران را هدایت کند تا اطمینان یابد که شیوه‌های ذخیره‌سازی داده‌ها (شامل حق اشتراک داده‌های شخص سوم) محدودیت جمع‌آوری داده‌ها را پشتیبانی می‌کند.
گزارش	[ارزش ۳] بدنهٔ حاکمیت باید مدیران را برای استفاده از ابزار و فناوری‌های لازم هدایت کند تا اطمینان یابد که می‌توان ارزش کامل داده‌ها را استخراج کرد.	[ریسک ۳] بدنهٔ حاکمیت باید اهمیت زمینه داده‌ها، از جمله هنجارهای فرهنگی و تفسیرهای نادرست بالقوه آن را در کل برقرار کند.	[تنگنای ۳] بدنهٔ حاکمیت باید اهمیت ارتباط بین داده‌ها و تنگناهای آن را تعیین کند، مخصوصاً اگر داده‌ها از مجموعه داده‌های مختلف جمع‌آوری شوند.
تصمیم	[ارزش ۴] بدنهٔ حاکمیت باید اطمینان یابد که مرزبندی داده برای سازمان با خط‌مشی داده‌های آن شامل رفتارهایی، همچون: شیوه‌های دسترسی به داده‌ها، تصمیم‌گیری دربارهٔ فعال‌سازی داده‌ها و یادگیری سازمانی از فرآیند تصمیم‌گیری همراستاست.	[ریسک ۴] باید داده‌ها و قالب مناسب برای تصمیمات خودکار یا تصمیمات انسانی در یک گزارش ارائه شوند. ضمن باقی‌ماندن پاسخگویی و تعهّدپذیری این تصمیمات، بدنهٔ حاکمیت باید مسئولیت‌های تصمیم‌گیری در سطح قابل‌قبول ریسک داده، به طرز مناسبی تفویض کند.	[تنگنای ۴] برونداد فرآیند تصمیم‌گیری، به عنوان داده جدید، ارزش، ریسک و تنگناهای خود را دارد و بدنهٔ حاکمیت باید انتظارات را برای فرآیند تصمیم‌گیری و مسئولیت‌های مرتبط تنظیم کند.

توزیع	[ارزش ۵] بدنهٔ حاکمیت باید خط‌مشی‌ای برای توزیع داده‌ها ایجاد کند تا اجازه دهد برنامه راهبردی سازمان را برآورده کند.	[ریسک ۵] بدنهٔ حاکمیت باید اطمینان یابد که مدیران اقدامات واپایشی کافی برای جلوگیری از توزیع نامناسب، پیاده‌سازی کرده‌اند.	[تنگنای ۵] بدنهٔ حاکمیت باید اطمینان یابد که حقوق توزیع مناسب پیاده‌سازی شده‌اند و توسط شخص سوم رعایت می‌شوند.
وارهایی	[ارزش ۶] بدنهٔ حاکمیت باید خط‌مشی‌هایی را تصویب کند تا امکان وارهایی داده‌ها را آنگاه که دیگر ارزشی ندارند یا نمی‌شود برای مدت طولانی‌تری نگهداری‌شان کرد، فراهم آورند.	[ریسک ۶] بدنهٔ حاکمیت باید مدیران را در به‌کارگیری فرآیندی مناسب برای وارهایی داده‌ها هدایت کند؛ فرآیندی که واپایش‌هایی همچون: نابودی ایمن و همیشگی داده‌ها را در خود دارد.	[تنگنای ۶] بدنهٔ حاکمیت باید الزام‌های مربوط به نگهداری و وارهایی داده‌ها را پایش کند و از به‌کارگیری فرآیندهای کافی اطمینان یابد.

کتابنامه

[۱] استاندارد ملی ایران شماره ۱۳۲۴۵: سال ۱۳۸۹، مدیریت ریسک- اصول و رهنمودها

[۲] استاندارد ملی ایران شماره ۱۷۶۴۳: سال ۱۳۹۲، فن‌آوری اطلاعات -فنون امنیتی -چارچوب کاری حریم خصوصی

[۳] استاندارد ملی ایران شماره ۱۹۴۷۶: سال ۱۳۹۳، استاندارد مدیریت ریسک-راهنمایی برای اجرای استاندارد ملی ایران شماره ۱۳۲۴۵

[4] ISO/IEC 38500, Information technology — Governance of IT for the organization

یادآوری- استاندارد ملی ایران شماره ۱۲۰۴۷: سال ۱۳۹۵، فناوری اطلاعات -حاکمیت فناوری اطلاعات (IT) برای سازمان، با استفاده از استاندارد2008: ISO/IEC 38500 تدوین شده است.

[5] ISO/IEC/TS 38501, Information technology — Governance of IT — Implementation Guide

[6] ISO/IEC/TR 38502, Information technology — Governance of IT — Framework and model

یادآوری- استاندارد ملی ایران شماره ۲۰۱۲۵: سال ۱۳۹۵، فناوری اطلاعات -حاکمیت فناوری اطلاعات -چارچوب و مدل، با استفاده از استاندارد ISO/IEC/TR 38502 :2014 تدوین شده است.

[7] ISO/IEC 17788:2014, Information technology — Cloud computing — Overview and vocabulary

[8] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

[9] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

[10] ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[11] ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[12] ISO/IEC 20546, Information technology — Big data — Definition and vocabulary

[13] ISO/IEC 20889, Information technology — Security techniques — Privacy enhancing data deidentification techniques

[14] “Framework for Improving Critical Infrastructure Cybersecurity” by National Instituteof Standards and Technology, USA.

[15] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf