به نام خدا

به اشتراک گذاری و آزادسازی داده ها

بخش اول - بررسی استانداردها

تهیه کننده: زهرا علوی‌کیا و مریم شبرو

مرکز نوآوری و توسعه فناوری اطلاعات، ارتباطات و امنیت سایبری

تاریخ: آذرماه ۱۴۰۱

پیشگفتار

دولت‌ها و کسب‌وکارها در سراسر جهان در حال جمع‌آوری و ذخیره‌سازی حجم عظیمی از داده‌ها هستند که در صورت آزادسازی دسترسی به این داده‌ها، آثار اقتصادی و اجتماعی قابل توجهی را به همراه می‌آورد. طی سال‌های اخیر کشورهای زیادی برنامه‌هایی را برای ایجاد دسترسی و آزادسازی داده‌ها اجرایی کرده‌اند که از آن میان می‌توان به قوانین انتشار عمومی داده در اتحادیه اروپا و یا مختص صنعت برق در وزارت انرژی آمریکا اشاره کرد.

داده باز به عنوان یکی از اصول هشتگانه دولت باز مطرح شده است که در صنایع مختلف مالی، سلامت، حمل و نقل، انرژی، آموزش و غیره به صورت بالقوه می‌تواند ارزش اقتصادی قابل توجهی ایجاد نماید. با توجه به رویکرد داده باز در دنیا نیاز است که داده‌های منتشر شده به راحتی قابل احصا بوده، در فرمت‌های قابل اصلاح و قابل خواندن با ماشین باشند، مجوز استفاده و توزیع مجدد داشته باشند و بدون هیچ هزینه‌ای در اختیار کاربران قرار گیرند. این الزامات دقیقا همان تعریف داده باز است که در صورت عدم تحقق، داده باز بودن عملا وجود نخواهد داشت. برای آزادسازی و دسترسی به داده‌های وزارت نیرو لازم است در ابتدا فهرستی از الزامات فنی و حقوقی مورد نیاز به عنوان الزامات داده باز تهیه شود. در تهیه این الزامات موضوعاتی از جمله شناسایی و اولویت‌بندی داده‌های وزارت نیرو جهت انتشار (برحسب میزان ارزش‌آفرینی آن‌ها) و شناسایی دارندگان آن‌ها، تفکیک داده‌های باز از داده‌های خصوصی، امنیت و حفاظت از داده‌ها، حساسیت داده‌ها، کیفیت و صحت داده‌ها، سطح دسترسی به داده‌ها، سوابق مدیریت داده‌ها، آماده‌سازی داده‌ها برای انتشار (شامل عنوان و مشخصات داده، قالب داده، تاریخ، تعیین سطح دسترسی، ناشر، مجوز، تاریخ بروزرسانی،...) و الزامات فنی بستر مورد نیاز برای انتشار داده‌ها مورد توجه قرار می‌گیرند.

ارائه نظام و الزامات فنی–حقوقی برای آزادسازی و دسترسی به داده‌های وزارت نیرو به عنوان یک توانمندساز اصلی در تغییر فضای کسب‌وکار و تسهیل آن محسوب می‌گردد که اثرات مستقیم و غیرمستقیمی را در ایجاد منافع اقتصادی و کسب‌وکارهای جدید، بهبود کارایی و اثربخشی خدمات عمومی، تصمیم‌گیری و اشتراک بهتر اطلاعات و افزایش شفافیت به همراه می‌آورد. در این راستا در قالب پروژه «**تدوین سند راهبردی حکمرانی داده در وزارت نیرو و راهبری عملیاتی نمودن آن در ستاد وزارت نیرو**» مطالعه‌ای به منظور بررسی استانداردها و مطالعه الگوبرداری در زمینه حکمرانی و آزادسازی داده‌ها، توسط همکاران مرکز نوآوری و توسعه فناوری اطلاعات، ارتباطات و امنیت سایبری خانم‌ها زهرا علوی کیا و مریم شبرو انجام شده که نتایج این مطالعه در قالب دو مجلد ارائه شده است. این گزارش به بررسی استانداردها اختصاص یافته است.

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

۱- مقدمه

در این گزارش، استانداردهایی که شمایی کلی از موضوعات قابل طرح در حکمرانی داده و آزادسازی داده را مطرح کرده‌اند به اجمال مرور می‌شوند و در انتها، دسته‌بندی از موضوعات مختلف حکمرانی داده در ابعاد مختلف و استانداردهای مرتبط با هر موضوع ارائه می‌شوند.

۲- چارچوب داده باز در شهرهای هوشمند (ITU-T Y.4461)

۲-۱- هدف

در این راهنما چارچوب داده باز در شهرهای هوشمند و با هدف توسعه به اشتراک‌گذاری داده بین نهادهای مختلف در شهر هوشمند تعریف می‌شود. اهداف این راهنما شامل موارد زیر می‌شود:

- مفهوم داده باز در شهرهای هوشمند
- مزایای داده باز در شهرهای هوشمند
- مراحل اصلی آزادسازی داده در شهرهای هوشمند
- نقش‌ها و وظایف برای آزادسازی داده در شهرهای هوشمند
- چارچوب داده باز در شهرهای هوشمند
- الزامات و توصیه‌های آزادسازی داده در شهرهای هوشمند

۲-۲- توافقات و قراردهای نوشتاری در این سند

در این سند (راهنما):

- کلید واژه‌های "لازم است که[1]" نیازمندی را بیان می‌کند که باید (must) موکداً دنبال شود و در صورت ادعای مطابقت با این سند، هیچ‌گونی تخطی و انحرافی از آن مجاز و قابل قبول نیست.

[1] Is required to

– کلید واژه‌های "توصیه می‌شود[1]" نیازمندی را بیان می‌کند که توصیه می‌شود اما به طور قطع الزام نمی‌شود. بنابراین برای ادعای تطابق با این سند، اجرای این نیازمندی (شرط) مورد نیاز نیست.

– کلیدواژه‌های "می‌تواند به صورت اختیاری[2]" و "ممکن است[3]" یک نیازمندی اختیاری مجاز را بدون هیچ‌گونه توصیه‌ای بیان می‌کنند. این مفاهیم به معنای این نیست که فروشنده باید گزینه یا ویژگی‌هایی را در پیاده‌سازی‌های خود در نظر بگیرد که می‌توانند به صورت اختیاری توسط اپراتور/ ارائه‌دهنده خدمات شبکه فعال شوند. در عوض، فروشنده ممکن است به صورت اختیاری این ویژگی‌ها را ارائه دهد و در عین حال ادعای تطابق با مشخصه‌های این سند را هم داشته باشد.

۲-۳- مفهوم داده باز در شهرهای هوشمند

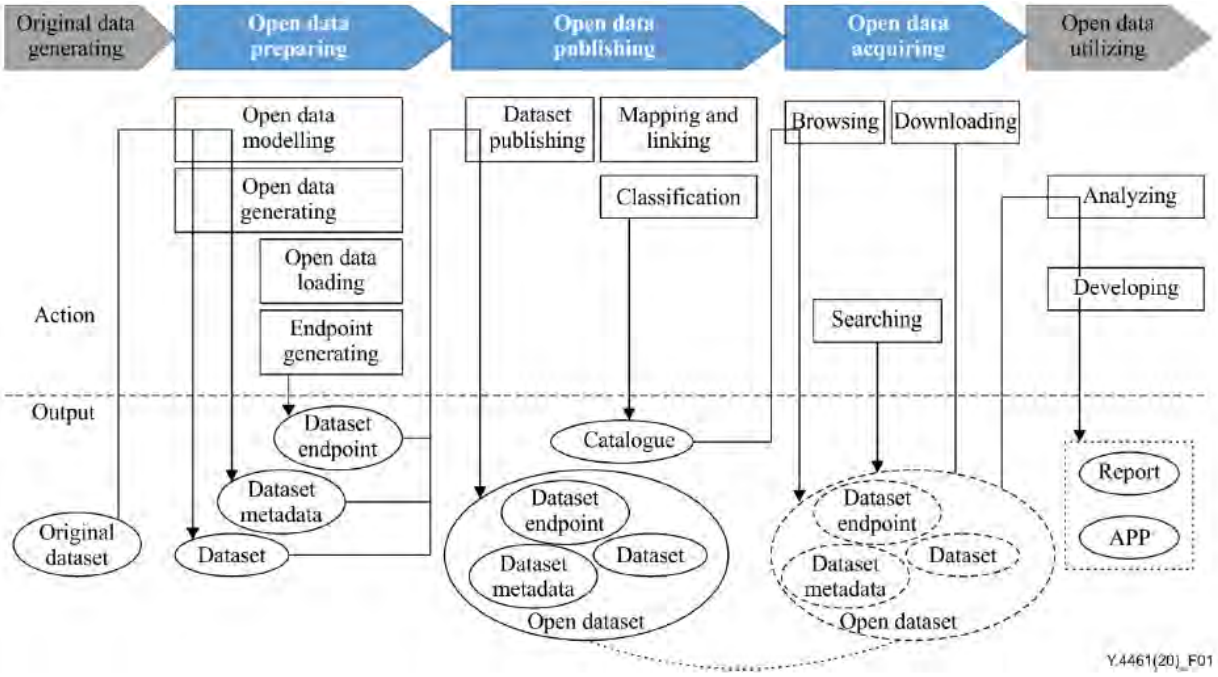
داده باز در شهرهای هوشمند به داده‌های سازمان‌ها و اشخاصی اشاره دارد که به صورت قابل خوانش توسط ماشین در اختیار عموم قرار داده می‌شود. این داده‌ها در دسترس عموم قرار دارند/ توسط عموم قابل مشاهده هستند، به صورت آزادانه قابل استفاده هستند، می‌توان آن‌ها را دوباره استفاده کرد، دوباره منتشر کرد و یا توسط هر شخص دیگری توزیع شوند [ISO 5127]. سازمان‌های مستعد انتشار داده باز شامل دولت‌ها، شرکت‌ها، سازمان‌های غیردولتی (سازمان‌های مردم نهاد) و غیره می‌شوند.

داده‌های قابل خوانش توسط ماشین[4] به داده‌هایی در شهرهای هوشمند گفته می‌شود که دیجیتالی شده‌اند و قابلیت بازیابی، درک و پردازش توسط سیستم‌های اطلاعاتی نظیر رایانه، تلفن هوشمند، و ... را دارند. داده‌ها باید (should) به جای روش‌های کاغذی به صورت دیجیتالی بازیابی شوند. همچنین داده‌ها باید به راحتی از طریق اینترنت قابل مشاهده و دستیابی باشند و به دفاتر دولتی یا کتابخانه‌ها محدود نشوند. داده‌های قابل خوانش با ماشین اغلب دارای قالب‌هایی مانند XML، CSV/ متن، KML/ KMZ، JSON و ... . قالب‌هایی مانند PDF که به سادگی توسط ماشین فهمیده و پردازش نمی‌شوند، قالب مناسبی برای داده باز محسوب نمی‌شود. داده‌های باز در شهرهای هوشمند شامل انواع قالب داده ساختاریافته مانند text و document و داده غیرساختاریافته مانند تصویر، صدا و ویدئو می‌شوند. همچنین داده‌های استریم نیز می‌توانند داده باز محسوب شوند. (مباحث داده باز در شهر هوشمند شامل حوزه‌های مختلفی مانند محیط زیست، کشاورزی، حمل‌ونقل، آموزش، انرژی، سلامت، دولت، علوم و تحقیقات، جغرافیا و ... می‌شود.)

[1] Is recommended
[2] Can optionally
[3] May
[4] Machine readable data

۲-۴- مراحل اصلی آزادسازی داده در شهر هوشمند

مراحل اصلی آزادسازی داده در شهرهای هوشمند شامل پنج مرحله، تولید داده اولیه[1]، آماده‌سازی داده باز[2]، انتشار داده باز[3]، اکتساب داده باز[4] و بهره‌برداری و بکارگیری داده باز[5] می‌شوند. در شکل ۱، اقدامات و خروجی‌های هر مرحله نشان داده شده است. در مرحله ۱، داده اولیه (اصلی) تولید می‌شود که شامل انواع مختلفی از داده مانند داکیومنت، تصویر، صوت، ویدئو و استریم می‌شود. در مرحله آماده‌سازی داده، داده برای انتشار آماده می‌شود. هدف مرحله انتشار داده باز، ایجاد قابلیت جستجو و دسترسی به داده برای عموم است. در مرحله اکتساب داده، مشتریان می‌توانند داده مورد نظر خود را جستجو و دریافت نمایند. در نهایت در مرحله بهره‌برداری و بکارگیری داده، داده برای خلق ارزش در شهرهای هوشمند مورد تحلیل و توسعه قرار می‌گیرد. جزئیات مراحل تولید داده اولیه و بکارگیری آن جهت خلق ارزش خارج از محدوده این سند ITU است.

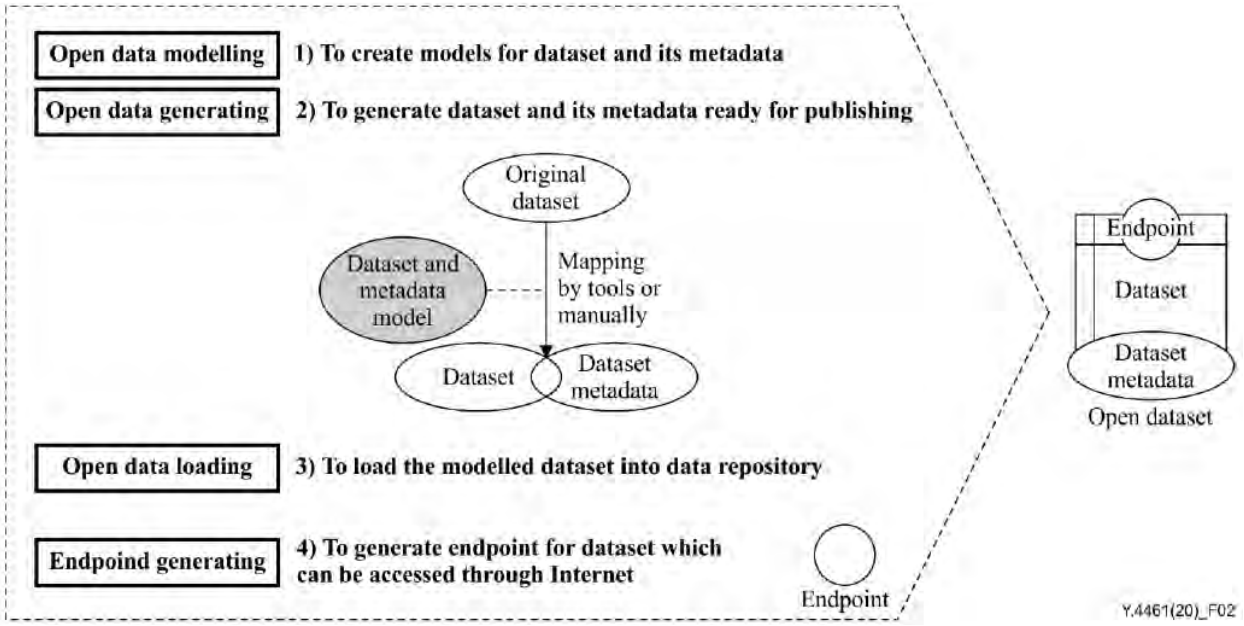


شکل ۱- مراحل اصلی آزادسازی داده در شهرهای هوشمند.

[1] Original data generating
[2] Open data preparing
[3] Open data publishing
[4] Open data acquiring
[5] Open data utilizing

۲-۴-۱- مرحله آماده‌سازی داده باز

این مرحله شامل ۴ گام مدل‌سازی داده باز[1]، تولید داده باز[2]، بارگذاری داده باز[3] و ایجاد (تولید) نقاط انتهایی[4] (نقاط دسترسی) می‌شود که در شکل ۲ آورده شده‌اند.



شکل ۲- مرحله آماده‌سازی داده باز

۲-۴-۱-۱- مدل‌سازی داده باز

هدف از مدل‌سازی داده باز ایجاد مدل‌هایی برای دیتاست[5] و متادیتا (فراداده[6]) آن است. این مرحله شامل مدل‌سازی متادیتا و دیتاست می‌شود. دیتاست به داده‌ای گفته می‌شود که می‌تواند دانلود و پس از انتشار برای دفعات متعدد مورد استفاده قرار گیرد. متادیتا، داده‌ای است که داده‌های دیگر را برای سهولت فهم، استفاده و مدیریت داده‌ها توسط انسان یا کامپیوترها توصیف می‌کند .[b-ITU-T FG-SSC Anon.]

[1] Open data modeling
[2] Open data generating
[3] Open data bading
[4] Endpoint generating
[5] Dataset
[6] Metadata

در مدل‌سازی دیتاست، یک ساختار با قابلیت خوانش ماشین برای دیتاست آماده انتشار تعریف می‌شود. در این ساختار، داده هم از ساختار نحوی[1] و هم از دیدگاه معنایی[2] یکپارچه می‌شوند. مدل دیتاست شامل اطلاعاتی مانند عنوان، ترتیب، نوع، توضیحات و غیره می‌شود. همچنین در صورت پشتیبانی از معناشناسی، از توضیحات معنایی داده مانند ontologies (هستی‌شناسی یا علم اطلاعات داده) هم استفاده می‌شود (برای مثال [b-ITU-T Y4500.12]).

ممکن است مدل‌های دیتاست متفاوتی برای دیتاست‌های حوزه‌های مختلف تعریف شود (برای مثال کشاورزی، آموزش، گردشگری و غیره) که برای توصیف هر یک از آن‌ها اصطلاحات مشخصی به کار گرفته می‌شود. همچنین مدل‌های دیتاست یک حوزه ممکن است یکسان باشند و یا با توجه به اینکه توسط اپراتورهای مختلف داده باز ارائه می‌شوند، متفاوت باشند.

در مدل‌سازی داده ممکن است مدلی برای داده‌های غیرساختاریافته مانند تصویر، صوت و یا استریم در نظر گرفته نشده باشد، اما برای تسهیل فهم داده باز برای انسان‌ها و ماشین‌ها، یک مدل متادیتا برای تمام انواع دیتاست آماده به انتشار نیاز است. همانطور که در بخش قبل توضیح داده شد، مدل‌سازی متادیتا دربردارنده اطلاعات توصیفی از دیتاست‌های آماده برای انتشار است. مدل متادیتا دربرگیرنده موضوعاتی مانند اطلاعات پایه (برای مثال، عنوان، موضوع، کلیدواژه، توضیحات و غیره)، اطلاعات زمانی-مکانی (برای مثال تاریخ ایجاد، تاریخ انتشار، محدوده پوشش، پوشش جغرافیایی و غیره)، خاستگاه یا منشاء اطلاعات (مانند سازمان انتشاردهنده داده، شخص پاسخگو و غیره)، اطلاعات اداری (به عنوان مثال نسخه یا ورژن، مدت اعتبار و غیره) و اطلاعات ساختاری مدل دیتاست (مانند عنوان، ترتیب، نوع، توضیحات و غیره) است. متادیتا به جستجوی سریعتر و راحتتر مشتریان داده و همچنین افزایش کارایی ماشین در فهم و پردازش داده‌ها کمک می‌کند.

۲-۴-۱-۲- تولید داده باز

هدف این گام، تولید دیتاست و متادیتا آن برای انتشار مطابق با مدل‌های استخراج شده در گام قبل است. در این گام، دیتاست اصلی (اولیه) به دیتاست و متادیتای مدل شده نگاشت می‌شوند که این کار می‌تواند هم به طور خودکار (از طریق ابزار) و هم به صورت دستی انجام پذیرد.

توجه ۱: یک دیتاست واحد را می‌توان به قالب‌های مختلف تولید کرد برای مثال فرمت‌های csv، rdf و xml برای داکیومنت‌ها و avi، mkv و rmvb برای ویدئو.

توجه ۲: پردازش‌های گمنام‌سازی باید (should) در صورت نیاز در طول فرآیند تولید داده‌های باز انجام پذیرد.

[1] Syntax
[2] Semantic

۲-۴-۱-۳- بارگذاری داده باز

در این گام دیتاست‌های مدل‌شده و متادیتاهای آن‌ها در یک مخزن داده بارگذاری می‌شوند به نحوی که مشتریان (مصرف‌کنندگان) بتوانند از طریق اینترنت به آن‌ها دسترسی پیدا کنند.

۲-۴-۱-۴- تولید (ایجاد) نقطه انتهایی

هدف این گام ایجاد نقاط دسترسی برای مشتریان به منظور دستیابی به داده باز مورد درخواستشان است. نمونه‌هایی از این نقاط دسترسی عبارتند از: URL دانلود برای دیتاست، URL دسترسی برای داده استریم، و API برای تسهیل به کارگیری و پردازش داده باز برای ماشین‌ها.

توجه: ممکن است چندین نقطه دسترسی برای یک دیتاست برای مثال به منظور نمایش فرمت‌های مختلف پیشنهاد شود.

۲-۴-۲- مرحله انتشار داده باز

مرحله انتشار داده باز از سه گام انتشار دیتاست[1]، نگاشت و پیوند[2] ، و طبقه‌بندی (دسته‌بندی)[3] تشکیل شده است (شکل ۳).

۲-۴-۲-۱- انتشار دیتاست

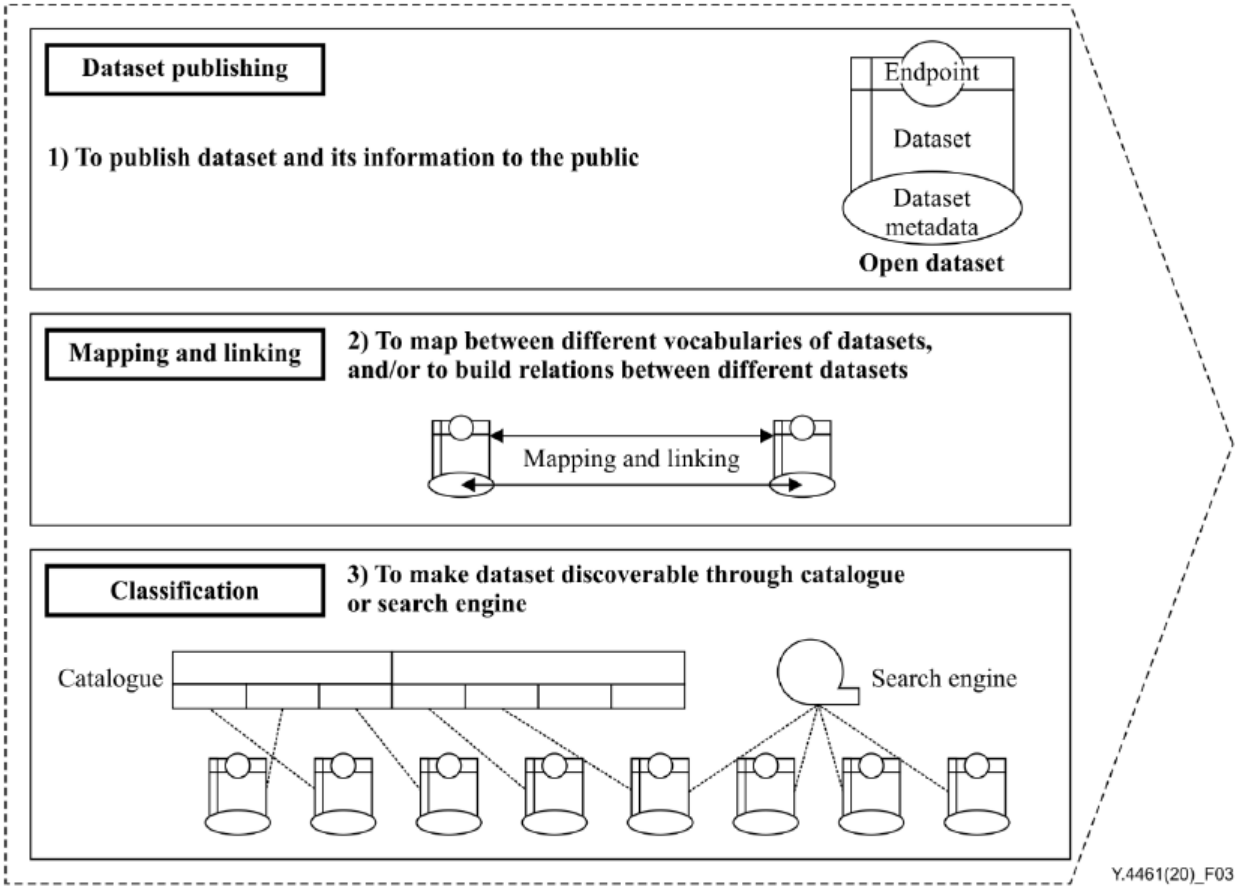
هدف این گام انتشار دیتاست و قراردادن اطلاعات مرتبط با آن برای عموم است. این اطلاعات شامل متادیتا و اطلاعات نقاط انتهایی است. دیتاست از طریق نقاط انتهایی منتشرشده قابل دسترس است.

۲-۴-۲-۲- پیوند و نگاشت

نگاشت با هدف یکپارچه‌سازی معناشناسی (semantic) دیتاست‌هایی است که از منابع مختلف جمع‌آوری شده‌اند (در دیتاست‌های منابع مختلف ممکن است از مدل‌های داده‌ی متفاوتی استفاده شده باشد). در این حالت، با رویکردهایی مانند نگاشت واژگان بین دیتاست‌های مختلف، تلاش می‌شود انطباق معنایی بین اطلاعات کلیدی دیتاست‌ها حفظ شود. این گام منجر به افزایش تعامل‌پذیری داده‌های باز و جستجوی موثرتر آن‌ها می‌شود.

در پیوند (لینک زدن)، ارتباط بین دیتاست‌ها با یکدیگر ایجاد می‌شود تا مشتریان (متقاضیان داده) بتوانند دیدی جامع از دیتاست‌های باز مرتبط با هم داشته باشند. ارتباط و منطق بین دیتاست‌های مختلف با روش‌ها و رویکردهایی مانند ایجاد پیوند مبتنی بر کلیدواژه‌ها[4]، ایجاد پیوند مبتنی بر واژگان[5] و ... انجام می‌گیرد

[1] Dataset publishing
[2] Mapping and linking
[3] Classification
[4] Interlinking based on keywords
[5] Interlinking based on vocabularies



شکل ۳- مرحله انتشار داده باز

۲-۴-۲-۳- طبقه‌بندی (کلاس‌بندی)

در این گام داده‌ها به منظور شناسایی (کشف) در موتورهای جستجو و کاتالوگ[1]، طبقه‌بندی می‌شوند. طبقه‌بندی دیتاست، امکان فیلترکردن داده‌باز را براساس مشخصه‌هایی مانند ناشر، موضوع، تاریخ انتشار و قالب برای مشتریان فراهم می‌کند.

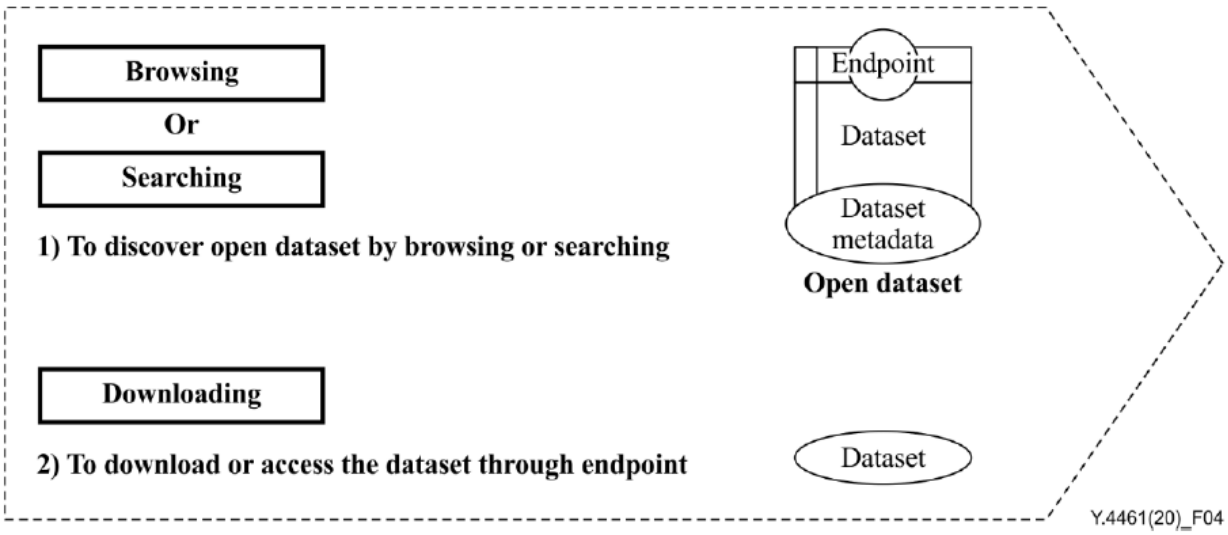
در کاتالوگ، نمایه (ایندکس[2]) داده باز به متقاضیان داده (مشتریان) نمایش داده می‌شود. در این بخش، مجموعه‌هایی از دیتاست‌های باز براساس معیارهای مختلف مانند موضوع (به عنوان مثال، اقتصاد، محیط زیست، آموزش و غیره)، سناریو (به عنوان مثال، آموزش و اشتغال، ازدواج و فرزندآوری، بازنشستگی و غیره)، و منبع (به عنوان مثال، وزارت دولت، سازمان‌ها و شرکت‌ها–NGO) طبقه‌بندی می‌شوند. همچنین، اطلاعاتی از دیتاست شامل متادیتای دیتاست و نقاط انتهایی جهت دسترسی به دیتاست در کاتالوگ موجود است.

[1] Catalogue
[2] Index

موتور جستجو به مشتریان داده کمک می‌کند تا داده‌های باز مورد نظر را به کمک کلیدواژه‌ها پیدا کنند. همچنین نتیجه جستجو را می‌توان با به کارگیری روش‌های پیوند و نگاشت دقیق‌تر کرد.

۲-۴-۳- مرحله دستیابی به (اکتساب) داده باز

این مرحله شامل سه گام مرور عناوین[1]، جستجو[2] و دانلود (بارگیری)[3] است که در شکل ۴ نشان داده شده است.



شکل ۴- مرحله اکتساب (دستیابی به) داده باز

عملیات مرور و جستجو به متقاضیان داده (مشتریان) کمک می‌کنند تا به راحتی دیتاست‌های مورد نیاز خود را کشف کنند. پس از یافتن اطلاعات دیتاست، مشتری قادر به مشاهده اطلاعات توصیفی از دیتاست از طریق متادیتای آن است، همچنین امکان دسترسی به دیتاست از طریق نقاط انتهایی آن نیز برای مشتری فراهم می‌شود تا دیتاست مورد نظر را دانلود کند یا لینک دسترسی به دیتاست (برای مثال داده استریم) را دریافت کند.

[1] Browsing
[2] Searching
[3] Downloading

۲-۵- نقش‌ها و اقدامات اصلی برای آزادسازی داده در شهرهای هوشمند

۲-۵-۱- نقش‌های کلیدی داده باز در در شهرهای هوشمند

براساس مراحل اصلی آزادسازی داده که در بخش‌های قبلی توضیح داده شد، سه نقش اصلی ارائه‌دهنده داده باز[1]، ناشر داده باز[2]، و مشتری داده باز[3] مشخص در اکوسیستم شهرهای هوشمند مشخص شده است.

ارائه‌دهنده داده باز مسئول آماده‌سازی دیتاست، ارائه اطلاعات آماده شده از دیتاست (منظور اطلاعات متادیتا و نقاط انتهایی است)، و در صورت لزوم دیتاست آماده به ناشر داده باز است.

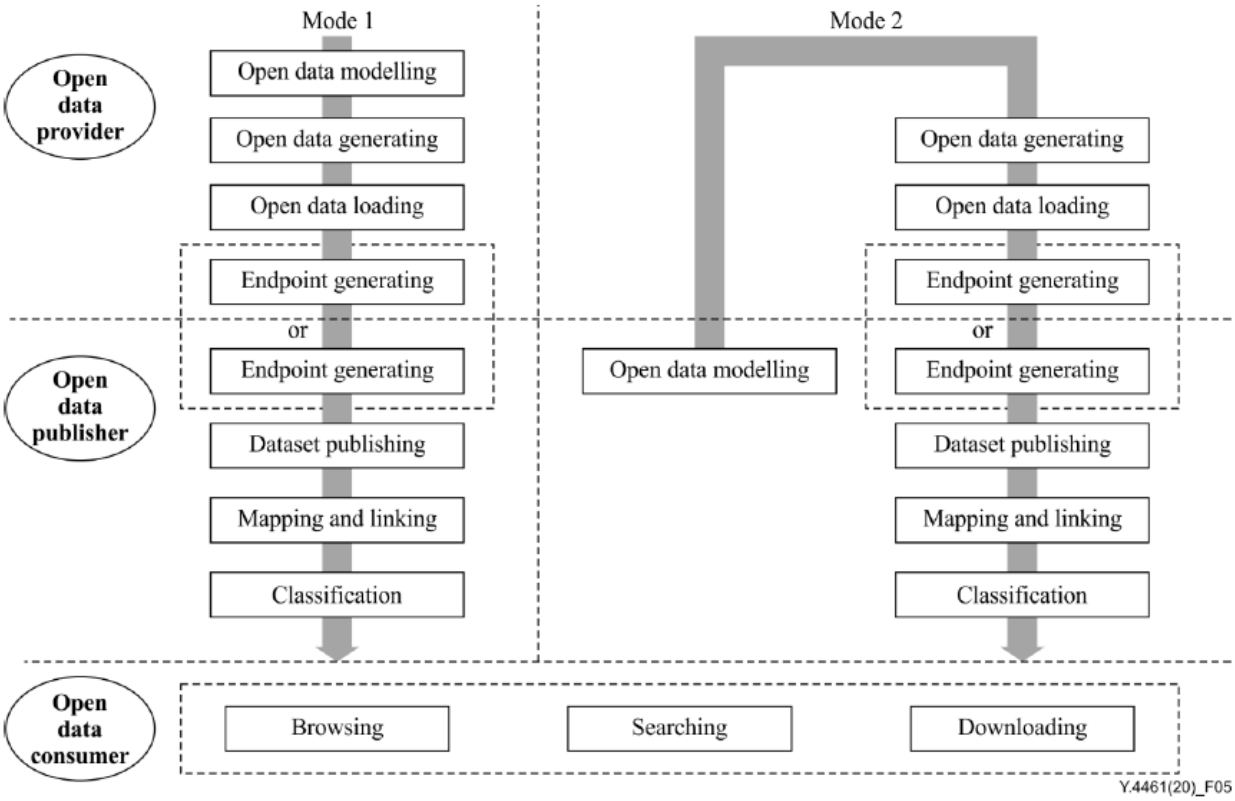
ناشر داده باز مسئول انتشار دیتاست‌ها، ایجاد قابلیت کشف و دسترس‌پذیری آن‌ها برای عموم است.

مشتری داده باز قادر به دریافت داده‌ها از طریق مرور، جستجو و دانلود(بارگیری) است. مشتریان داده باز شامل مشتریان شخصی داده باز[4] و توسعه‌دهندگان داده باز[5] می‌شوند. مشتریان شخصی داده باز، از داده‌ها برای بهبود کیفیت زندگی، و توسعه‌دهندگان برای ارائه خدمات ارزش افزوده استفاده می‌کنند.

۲-۵-۲- اقدامات کلیدی آزادسازی داده در شهرهای هوشمند

در شکل ۵، اقدامات کلیدی هر نقش داده باز در شهرهای هوشمند براساس دو حالت مختلف آزادسازی داده نشان داده شده است (مستطیل‌های نقطه‌چین اقداماتی را نشان می‌دهد که می‌تواند توسط نقش مورد نظر انجام پذیرد یا نپذیرد).

[1] Open data provider
[2] Open data publisher
[3] Open data consumer
[4] Individual open data consumer
[5] Open data developer



شکل ۵- اقدامات اصلی داده باز در شهرهای هوشمند

در حالت ۱ (mode 1)، مدل‌سازی داده باز در سمت ارائه‌دهنده داده باز انجام می‌گیرد. در این حالت ممکن است مدل دیتاست با توجه به ارائه‌دهنده آن متفاوت باشد که در این صورت لازم است که ناشر داده باز با استفاده از روش‌های نگاشت و پیوند، دیتاست‌ها را از نظر معناشناسی یکپارچه نماید.

در حالت ۲ (mode 2)، مدل‌سازی داده باز توسط ناشر داده باز انجام می‌گیرد. در این حالت، ارائه‌دهنده داده باز، دیتاست خود را مطابق مدل یکپارچه پیشنهاد شده توسط ناشر، تولید می‌کند که باعث تسهیل تعامل‌پذیری داده‌های باز از منابع مختلف می‌شود.

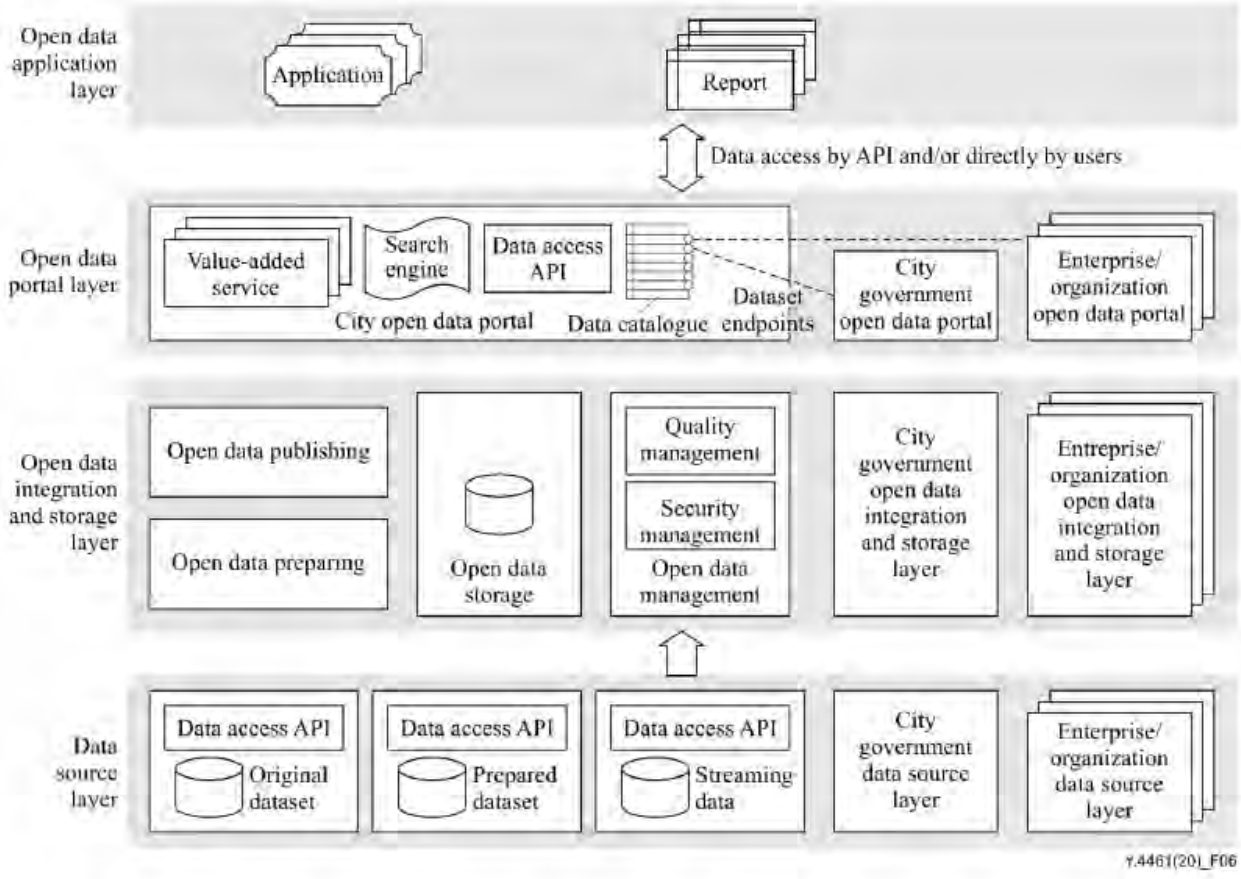
تولید نقاط انتهایی با توجه به محل مخزن قرارگیری دیتاست، می‌تواند در سمت ارائه‌دهنده یا ناشر داده باز انجام گیرد. برای مثال اگر دیتاست در سمت ارائه‌دهنده قرار گیرد، ارائه‌دهنده داده باز مسئول تولید نقطه (یا نقاط) انتهایی است (و برعکس).

مشتری داده باز می‌تواند داده مورد نیاز خود را با توجه به محل مخزن دیتاست، از ارائه‌دهنده یا ناشر داده باز دریافت کند.

در پیاده‌سازی‌ها، یک حالت ترکیبی نیز می‌تواند وجود داشته باشد که در آن مدل‌سازی داده می‌تواند در هر دوسمت ارائه‌دهنده و ناشر داده باز انجام پذیرد.

۲-۶- چارچوب داده باز در شهرهای هوشمند

چارچوب داده باز در شهرهای هوشمند از لایه‌های منبع داده[1]، ادغام و ذخیره داده باز[2]، پورتال داده باز[3]، و کاربرد داده باز[4] تشکیل شده است (شکل ۶).



شکل ۶- چارچوب داده باز در شهرهای هوشمند

[1] Data source layer
[2] Open data integration and storage layer
[3] Open data portal layer
[4] Open data application layer

۲-۶-۱- لایه منبع داده

لایه منبع داده شامل دیتاست اصلی (اولیه)[1]، دیتاست آماده[2] و داده استریم[3] (در صورت امکان) است.

منظور از داده اولیه داده‌ای است که به عنوان دیتاست باز، قبل از انتشار نیاز به آماده‌سازی دارد. از این رو لازم است داده اولیه به منظور آماده‌سازی در لایه ادغام (یکپارچه‌سازی) و ذخیره‌سازی بارگذاری شود. این لایه شامل مدل‌سازی داده باز، تولید داده باز، بارگذاری داده باز و تولید (ایجاد) نقاط انتهایی است که در بخش قبل در مورد آنها توضیح داده شد.

منظور از دیتاست آماده، داده‌ای است که آماده انتشار است و مطابق مدل داده باز تولید شده است. دیتاست آماده را می‌توان با توجه به سناریوهای تعیین شده به صورت محلی و یا در لایه ادغام و ذخیره‌سازی، ذخیره کرد.

بارگذاری (آپلود) منبع داده (شامل دیتاست اولیه و دیتاست آماده) می‌تواند به صورت دوره‌ای و/یا مبتنی بر وقوع رویداد صورت پذیرد. از push منبع داده در لایه ادغام و ذخیره‌سازی و / یا pull آن برحسب درخواست، پشتیبانی می‌شود.

دیتاست اصلی و دیتاست می‌توانند آماده از طریق روش‌هایی مانند API دسترسی داده و به صورت دستی بارگذاری شوند.

ارائه‌دهنده داده استریم مسئول تولید نقاط انتهایی و ارسال اطلاعات نقاط انتهایی (اتصال) به لایه ادغام و ذخیره‌سازی است (شامل زیرساخت عمومی داده باز برای شهر هوشمند و/ یا زیرساخت مستقل داده باز). همچنین امکان بارگذاری داده‌های استریم در لایه ادغام و ذخیره‌سازی از طریق API دسترسی داده وجود دارد.

۲-۶-۲- لایه ادغام (یکپارچه‌سازی) و ذخیره‌سازی داده باز

این لایه شامل توابع آماده‌سازی داده باز[4]، انتشار داده باز[5]، ذخیره‌سازی داده باز[6] و مدیریت داده باز[7] می‌شود.

همان‌طور که در بخش‌های قبلی توضیح داده شد، آماده‌سازی داده باز شامل مدل‌سازی داده باز، تولید داده باز، بارگذاری داده باز و تولید نقطه (نقاط) انتهایی می‌شود. در این بخش، از انتقال دیتاست اصلی به صورت بلادرنگ به دیتاست باز پشتیبانی می‌شود.

[1] Original dataset
[2] Prepared dataset
[3] Streaming data
[4] Open data preparing
[5] Open data publishing
[6] Open data storage
[7] Open data management

همچنین در این لایه (لایه ادغام و ذخیره‌سازی داده باز) در صورت درخواست، از ذخیره‌سازی نقاط انتهایی و ذخیره (ذخیره‌سازی در حافظه نهان)[1] و توزیع داده استریم به کاربران پشتیبانی می‌شود. به علاوه به کاربران یک پخش‌کننده رسانه (مدیا پلیر)[2] برای مشاهده داده استریم ارائه می‌شود.

توابع انتشار داده باز مطابق آنچه در بخش‌های قبلی توضیح داده شد، شامل انتشار دیتاست، پیوند و نگاشت، و طبقه‌بندی دیتاست‌ها می‌شود. این تابع به انواع داده باز پس از آماده‌سازی آن‌ها اعمال می‌شود.

تابع ذخیره‌سازی داده باز شامل ذخیره‌سازهای موقتی / حافظه نهان و دائمی می‌شود که از ذخیره‌سازی داده بر روی زیرساخت داده باز به صورت موقت یا دائمی براساس الزامات تعیین شده پشتیبانی می‌کند.

تابع مدیریت داده باز از دو بخش مدیریت کیفیت و امنیت تشکیل شده است. وظیفه تابع مدیریت کیفیت تضمین کیفیت داده باز بعد و قبل از انتشار است. کارکردهای مدیریت کیفیت شامل بررسی (وارسی) یکپارچگی[3] داده باز، به روز رسانی به موقع داده‌ها برحسب درخواست، اطمینان از ردیابی[4] داده‌های باز و غیره می‌شود. همچنین در صورت کاربرد، مسئول کنترل کیفیت خدمات (QoS) داده استریم است.

توابع مدیریت امنیت شامل صدور مجوز برای ارائه‌دهنده داده، محافظت از محرمانگی اطلاعات حساس با استفاده از فناوری مانند گمنام‌سازی و اعتبارسنجی داده باز می‌شود.

توجه: اگر خدمت ارزش افزوده شخص ثالث در پورتال داده باز در دسترس باشد، توابع مرتبط مانند مدیریت ارائه‌دهنده خدمت، مدیریت خدمات و انتشار آن‌ها نیز باید در لایه ادغام و ذخیره‌سازی پشتیبانی شوند.

۲-۶-۳- لایه پورتال داده باز

در این لایه، داده باز و خدمات مرتبط با آن به صورت قابل کشف در دسترس عموم قرار داده می‌شود. توابعی مانند کاتالوگ داده، موتور جستجو و خدمات ارزش افزوده در صورت کاربرد در این لایه قرار می‌گیرند (که از طریق API داده باز یا به خودی خود در اختیار کاربران قرار داده می‌شوند).

[1] Caching
[2] Media player
[3] Integrity
[4] Traceability

کاربران می‌توانند دیتاست مورد نظر خود را از طریق نقطه انتهایی آن دانلود نمایند. نقاط انتهایی داده‌های ارائه شده در پورتال (شامل پورتال عمومی داده باز شهر و پورتال اختصاصی داده باز) به مجموعه‌ی داده‌ها از زیرساخت محلی داده باز یا سایر زیرساخت داده باز اشاره دارد که باعث تضمین قابلیت تعامل داده‌های باز می‌شود.

خدمات ارزش افزوده شامل خدماتی مانند آمار و اطلاعات بصری‌سازی داده‌های باز و همچنین خدمات اشخاص ثالث[1] مانند برنامه‌های مبتنی بر داده‌های باز، گزارش‌های تحلیلی و غیره می‌شود.

۲-۶-۴- لایه کاربرد داده باز

کاربران از داده‌های باز برای ایجاد خدمات شهرهوشمند مانند برنامه‌های کاربردی و گزارشات تحلیلی استفاده می‌کنند. خدمات داده باز را می‌توان روی پورتال داده باز در دسترس عموم قرار داد که باعث افزایش ارزش و بهبود بکارگیری داده باز می‌شوند.

۲-۷- نیازمندی‌های کلی داده‌های باز در شهرهای هوشمند

۲-۷-۱- نیازمندی‌های (الزامات) مشترک داده باز در شهرهای هوشمند

۱. توصیه می‌شود دسترسی به داده باز بدون ثبت‌نام اجباری انجام پذیرد که در این حالت کاربران بدون نیاز به شناسایی می‌توانند از داده باز استفاده کنند.

توجه ۱: از یک سازوکار ثبت‌نام برای ارائه توابعی مانند ثبت اطلاعاتی از داده‌های بازدید شده توسط کاربران نیز می‌توان استفاده کرد که به شناخت بهتر علایق و اولویت‌های کاربران کمک می‌کند.

۲. لازم است دسترسی به داده باز بدون محدودیت زمان و مکان انجام پذیرد. لازم است دسترسی به این داده‌ها به راحتی از طریق اینترنت (در هرجا) امکان‌پذیر باشد و به دسترسی از طریق برخی مکان‌های محدود مانند کتابخانه‌ها یا دفاتر دولت محدود نشود. همچنین لازم است داده در هر زمانی در دسترس باشد.

۳. توصیه می‌شود از استفاده مجدد، انتشار مجدد و توزیع مجدد داده باز توسط کاربران پشتیبانی شود.

۴. توصیه می‌شود از ارائه داده باز و اطلاعات مرتبط با آن از طریق پورتال وب پشتیبانی شود تا دسترسی مردم به آن‌ها راحت باشد.

[1] Third parties

۵. توصیه می‌شود از ارائه داده باز و اطلاعات مرتبط با آن از طریق API(ها) پشتیبانی شود تا پردازش آن برای سیستم‌های اطلاعاتی آسان باشد.

۶. توصیه می‌شود از دسترسی به داده‌های تاریخ و زمان–واقعی پشتیبانی شود.

۷. توصیه می‌شود از جستجوی کلی {مرور} (browsing) داده باز بر حسب موضوع و/یا انواع متادیتا پشتیبانی شود.

۸. لازم است از توابع جستجوی داده باز به وسیله کلیدواژه‌ها پشتیبانی شود. توصیه می‌شود از توابع جستجوی مبتنی بر توصیف زمان طبیعی[1] پشتیبانی شود.

۹. توصیه می‌شود برای کمک به کاربران برای فهم بهتر داده‌ها از توابع بصری‌سازی داده‌ها[2] استفاده شود.

۱۰. توصیه می‌شود ابزارهای بصری‌سازی[3] داده را در اختیار کاربران قرار دهید تا هم به توسعه‌دهندگان در راستای ایجاد برنامه‌های کاربردی جدید کمک شود و هم کاربران بتوانند از طریق تحلیل داده و کشف بینش از آن برای برآوردن نیازمندی‌های خود بهره گیرند.

۱۱. توصیه می‌شود از برنامه‌های کاربردی (اپلیکیشن‌های) داده باز در پرتال (درگاه) وب پشتیبانی شود تا کاربران به راحتی بتوانند به مرور (browse)، جستجو (search) و استفاده از برنامه‌های کاربردی مورد نیاز بپردازند.

۱۲. توصیه می‌شود از یک سازوکار ثبت بازخورد (فیدبک) کاربران داده باز پشتیبانی شود. محتوای بازخورد ممکن است شامل نیازمندی‌های محتوای جدید داده باز، بهبود داده‌های موجود و غیره باشد.

۱۳. توصیه می‌شود انواع مختلف داده باز به یکدیگر لینک (پیوند) داشته باشند تا یافتن داده‌های مرتبط باهم به سادگی انجام پذیرد.

توجه ۲: داده‌های باز را می‌توان با استفاده از روش‌هایی مانند شناسه‌ها، برچسب‌گذاری‌ها و غیره به یکدیگر لینک (پیوند) داد.

۱۴. لازم است داده‌های باز قابلیت خوانش با ماشین[4] را داشته باشند تا توسط سیستم‌های اطلاعاتی قادر به بازیابی، فهم و پردازش باشند.

۱۵. توصیه می‌شود داده‌های باز در انواع مختلف شامل داده ساختاریافته (برای مثال CSV، XML و غیره) و داده‌های رسانه‌ای (برای مثال تصویر، صدا، ویدئو و غیره) ارائه شوند.

۱۶. توصیه می‌شود از توابع کاتالوگ به منظور طبقه‌بندی (دسته‌بندی) و نمایش بهتر داده‌های باز پشتیبانی شود.

[1] Natural language description
[2] Data visualization functions
[3] Visualization tools
[4] Machine-readable

۱۷. توصیه می‌شود از دسترسی به اطلاعات کاتالوگ از طریق یک API و/ یا درگاه وب پشتیبانی شود.

۱۸. توصیه می‌شود از توابع آماری و تحلیلی برای نمایش رفتار بازدیدکنندگان داده باز مانند نمایش موضوعات داغ داده باز در شهرهای هوشمند پشتیبانی شود.

۱۹. توصیه می‌شود از توسعه‌دهندگان نرم‌افزاری برای بارگذاری (آپلود) برنامه‌های کاربردی مرتبط با داده باز در شهرهای هوشمند یا پیوند (لینک) آن‌ها بر روی درگاه وب پشتیبانی شود.

۲۰. لازم است صحت[1] داده‌های باز تضمین شود. برای مثال صحت مواردی مانند شناسایی و حذف داده‌های غیرعادی[2] پس از فرآیند پاک‌سازی داده یا نگهداری داده‌های غیرعادی با ذکر توضیحات تضمین گردد.

۲۱. لازم است داده‌های باز منتشر و به روزرسانی شوند تا همواره نسخه به روز آن‌ها نگهداری شود.

۲۲. توصیه می‌شود تا حد امکان داده‌های باز شهرهای هوشمند در اختیار عموم قرار گیرد (ارائه شوند). در صورت عدم وجود داده مرتبط، ذکر توضیحات لازم است (need).

۲۳. توصیه می‌شود تا حد امکان داده اصلی ارائه شود تا کاربران بتوانند داده‌ها را مطابق ملاحظات خود تحلیل و پردازش کنند.

۲۴. توصیه می‌شود از داده‌های اصلاح شده با شرح تغییرات ایجاد شده پشتیبانی شود.پ

۲۵. لازم است اطلاعات مرتبط با داده باز مانند عنوان ارائه‌دهنده داده و تاریخ انتشار مشخص باشد تا ردیابی داده‌ها امکان‌پذیر باشد.

۲۶. توصیه می‌شود متادیتای داده باز شامل دیتاست‌ها و داده استریم ارائه شوند. توصیه می‌شود توضیحات متادیتا در قالب‌ها (فرمت‌های) قابل خوانش توسط ماشین و انسان در دسترس باشد.

۲۷. توصیه می‌شود از قابلیت همکاری[3] داده‌های باز که از زیرساخت‌های مختلف جمع‌آوری شده‌اند، پشتیبانی شود.

۲-۷-۲- امنیت و حریم خصوصی داده باز در شهرهای هوشمند

۱. لازم است شناسه (هویت)[4] و اعتبار[5] ارائه‌دهندگان داده باز قبل از ارائه یا بارگذاری (آپلود) داده باز در شهرهای هوشمند وارسی شوند (تأیید شوند).

[1] Accuracy
[2] Abnormal data
[3] Interoperability
[4] Identity
[5] Authority

۲. لازم است داده قبل از انتشار به صورت داده باز وارسی (تأیید و اعتبارسنجی) شود.

۳. لازم است از محرمانگی اطلاعات حساس هنگام انتشار داده باز در شهرهای هوشمند محافظت به عمل آید.

* در حوزه داده باز دو استاندارد Y.ODI تحت عنوان شناساگر داده باز در شهرهای هوشمند[1] (https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=13708) و همچنین استاندارد Y.4454 تحت عنوان تعامل‌پذیری پلتفرم‌ها برای شهرهای هوشمند[2] (https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=10815) توسط ITU در حال تدوین است.

۳- استاندارد ISO/IEC TR 38505-1: حکمرانی فناوری اطلاعات- حکمرانی داده‌ها قسمت 1: کاربرد استاندارد ISO/IEC 38500 در حکمرانی داده‌ها

۳-۱- هدف و دامنه کاربرد

هدف از تدوین استاندارد ISO/IEC 38505-1، ارائه راهنمایی برای اعضای بدنه حکمرانی سازمان‌ها (شامل صاحبان، مدیران، شرکا، مدیران اجرایی یا مشابه آن‌ها) به منظور استفاده اثربخش، کارا و قابل قبول داده‌ها در سازمان‌هایشان از طریق روش‌های زیر است:

- اعمال اصول حکمرانی و مدل ISO/IEC 38500 برای حکمرانی داده‌ها
- پیروی از اصول و شیوه‌های پیشنهاد شده در این استاندارد به منظور جلب اطمینان ذی‌نفعان برای حکمرانی قابل اعتماد داده‌های سازمان
- اطلاع‌رسانی و ارائه راهنمایی به بدنه‌ی حکمرانی در بکارگیری و حفاظت از داده‌های سازمانی
- ایجاد واژگان حکمرانی داده‌ها

[1] Open data indicator in smart cities
[2] Platforms interoperability for smart cities

در این استاندارد، حکمرانی داده‌ها به عنوان زیرمجموعه‌ای از حکمرانی فناوری اطلاعات تعریف می‌شود که خود حکمرانی فناوری اطلاعات، زیرمجموعه یا حوزه‌ای از حکمرانی سازمان و در مورد شرکت‌ها، حکمرانی شرکتی است.

۳-۲- حکمرانی خـوب داده‌ها

۳-۲-۱- فواید حکمرانی خوب داده‌ها

بدنه‌ی حکمرانی می‌تواند در موارد زیر پاسخگو و تعهدپذیر[1] باشد:

- 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

۳-۲-۲- مسئولیت‌های بدنه حکمرانی

- اعضای بدنه‌ی حکمرانی مسئول حکمرانی داده و متعهد به استفاده اثربخش، کارا و قابل قبول از داده‌ها در سازمان هستند.
- اختیار، مسئولیت‌پذیری، پاسخگویی و تعهدپذیری بدنه‌ی حکمرانی برای استفاده موثر، کارا و قابل قبول داده‌ها، از مسئولیت‌پذیری کلی حکمرانی سازمان و تعهدات آن به ذی‌نفعان خارجی از جمله تنظیم‌کنندگان مقررات ناشی می‌شود.
- تمرکز کلیدی نقش بدنه‌ی حکمرانی در حکمرانی داده این است که در حالی که ریسک را مدیریت می‌کند و به محدودیت‌ها توجه دارد بتواند اطمینان دهد که سازمان از طریق سرمایه‌گذاری در داده‌ها و فناوری اطلاعات ارزش مرتبط را به دست می‌آورد.
- بدنه‌ی حکمرانی 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 از داده‌ها، حریم خصوصی و احترام به دارایی فکر و اندیشه وجود دارد.

[1] Accountable

۳-۲-۳- بدنه حکمرانی و سازوکارهای نظارتی

– بدنه‌ی حکمرانی باید سازوکارهای نظارتی را برای حکمرانی داده‌هایی که با کسب‌وکارهای داده محور مرتبط هستند، ایجاد کند.

– بدنه‌ی حکمرانی باید درک روشنی از اهمیت داده‌ها در راهبردهای کسب‌وکار سازمان و همچنین ریسک راهبردی بالقوه سازمان برای استفاده از داده‌ها را داشته باشد (میزان توجه بدنه‌ی حکمرانی به داده‌ها باید مبتنی بر این عوامل باشد)

– بدنه‌ی حکمرانی باید اطمینان حاصل کند که اعضای آن و سازوکارهای حکمرانیی مربوطه (مانند ممیزی، مدیریت ریسک و کمیته‌های مربوط) و همچنین مدیران دانش و درک لازم از اهمیت داده‌ها را دارند.

– بدنه‌ی حکمرانی ممکن است کمیته‌ای فرعی ایجاد کند تا به کمک آن براستفاده‌ی سازمان از داده‌ها با دیدگاه راهبردی نظارت کند. نیاز به کمیته فرعی به اهمیت داده‌های سازمان و اندازه آن بستگی دارد.

– بدنه‌ی حکمرانی باید اطمینان دهد که چارچوب حکمرانیی مناسبی برای حکمرانی و مدیریت داده‌ها ایجاد شده است.

– بدنه‌ی حکمرانی باید اثربخشی سازوکارهای حکمرانی و مدیریت داده‌ها را با الزام فرآیندهایی مانند ممیزی و ارزیابی مستقل پایش کند تا اطمینان حاصل شود که حکمرانی مؤثر واقع شده است.

۳-۳- اصول، مدل و جنبه‌های حکمرانی خوب داده

استاندارد ISO/IEC 38505-1 بر پایه استاندارد ISO/IEC 38500 برای بررسی خاص داده‌ها و استفاده از آن‌ها توسط سازمان تدوین شده است.

براساس استاندارد ISO/IEC 38500، شش اصل حکمرانی خوب فناوری اطلاعات عبارتند از: مسئولیت‌پذیری، راهبرد، اکتساب، عملکرد، انطباق و رفتارانسانی. همچنین در این استاندارد چرخه « ارزیابی– هدایت– پایش» (EDM[1]) به عنوان مدلی برای حکمرانی فناوری اطلاعات ایجاد شده است.

برای به کارگیری اصول و مدل در حکمرانی داده ضروری است که جنبه‌های خاص داده‌های حکمرانیی برای راهنمایی بررسی شوند. جنبه‌های خاص داده‌های حکمرانیی در این استاندارد عبارتند از: ارزش، ریسک و تنگناها (محدودیت‌ها).

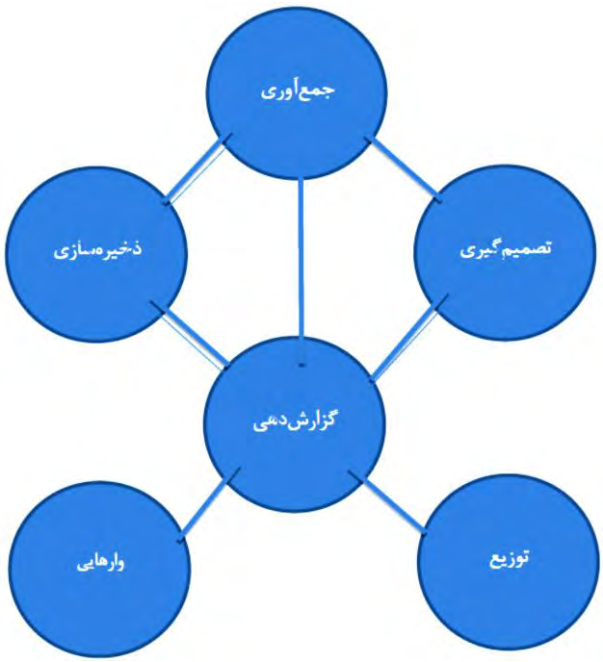
[1] Evaluate-Direct-Monitor

- **ارزش:** ارزش داده تا زمانی که توسط سازمان استفاده نشود، شناخته شده نیست. اصطلاح ارزش در این مورد شامل کیفیت و کمیت داده‌ها، بهنگام بودن آن‌ها[1]، هزینه ذخیره‌سازی، نگهداری، کاربری و وارهایی (دورریزی[2]) آن‌ها نیز می‌شود.
- **ریسک:** ریسک‌ها در مواردی شامل نقض داده‌ها، سودجویی از داده‌ها و استفاده نادرست از داده‌ها آشکار می‌شوند.
- **تنگناها (محدودیت‌ها):** محدودیت‌های داده 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. محدودیت‌های دیگری مانند تعهدات اخلاقی یا اجتماعی یا خط‌مشی‌های سازمانی نیز وجود دارند.

۳-۴- تعهدپذیری داده‌ها

۳-۴-۱- کلیات

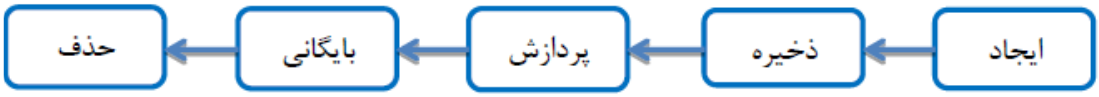
شکل ۷، حوزه‌های تعهدپذیری داده‌ها در یک سازمان را نشان می‌دهد.



شکل ۷- نقشه پاسخگویی و تعهدپذیری داده‌ها

[1] Timeliness
[2] Dispose

یادآور می‌شود این استاندارد بر حکمرانی داده متمرکز است که نباید با مدیریت داده اشتباه گرفته شود. در حالی که بدنه حکمرانی با اصول حکمرانی مشخص شده در بند قبل سروکار دارد، حوزه مدیریت داده‌ها با روش‌های تعریف‌شده‌ای برای پردازش داده‌ها و نیز سازوکارهایی برای اطمینان از محرمانگی، یکپارچگی و بازیافت داده‌ها مرتبط است. مثالی از چرخه عمر مدیریت داده‌ها در شکل ۸ نشان داده شده است.



شکل ۸- مثالی از چرخه عمر مدیریت داده‌ها

۳-۴-۲- 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. برخی از روش‌های ایجاد و جمع‌آوری داده عبارتند از: با استفاده از برنامه‌های کاربردی درون سازمانی یا به شکل خارجی از طریق وب‌سایت، برنامه کاربردی تلفن همراه یا برنامه‌های مشابه، تبادل داده‌های الکترونیکی (EDI[1]) یا دیگر فرآیندهای واسطه‌سازی، حسگرها، ...

۳-۴-۳- ذخیره‌سازی

فعالیت ذخیره شامل قرار دادن داده‌ها در جایی است که به لحاظ فیزیکی یا منطقی بتوان بازیابی کرد. این فعالیت افزاره‌های[2] ذخیره‌سازی درون سازمانی، برون سازمانی و مخزن‌های مجازی را در برمی‌گیرد (با استفاده از زیست‌بوم‌های رایانش ابر عمومی، هزینه‌های قابلیت‌های پردازش و ذخیره در مقیاس بزرگ بسیار کاهش می‌یابد). در هر صورت نظارت بر داده‌ها به عهده بدنه حکمرانی است.

۳-۴-۴- گزارش‌دهی

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

[1] Electronic Data
[2] Devices

۳-۴-۵- تصمیم‌گیری

فعالیت تصمیم‌گیری براساس بررسی گزارش و توسط افراد درون سازمانی یا به روش‌های خودکار انجام می‌شود.

– بدنه حکمرانی درباره‌ی تمام تصمیمات پاسخگو و تعهدپذیر بوده و باید اطمینان یابد که واپایش‌های (کنترل‌های) مناسبی برای آن‌ها وجود دارد و در صورت لزوم، مداخله‌های انسانی برای مقابله با هرگونه تعصبات، تبعیض یا نمایه‌سازی در فرآیند تصمیم‌گیری اعمال می‌شود.

بازخورد سودمندی داده‌ها (براساس تصمیمات اخذ شده از آن‌ها) به فرآیند جمع‌آوری و ایجاد داده‌ها باز می‌گردد.

۳-۴-۶- توزیع

فعالیت توزیع شامل استخراج یا رونوشت داده‌ها از طریق فعالیت گزارش‌دهی برای انتقال به طرف‌های خارجی است (این کار به دلایلی از جمله گزارش‌دهی به یک مقام مجاز حکمرانیی، فروش داده‌ها به یک شرکت تحقیقاتی یا تبلیغاتی، داده‌ها بخشی از کسب‌وکار سازمان باشند،..).

۳-۴-۷- وارهایی

فعالیت وارهایی معمولا شامل: شناسایی داده‌های دورریز از طریق انجام فعالیت گزارش‌دهی و سپس پاک کردن آن داده‌ها و همه‌ی رونوشت‌هایشان از انبار (مخزن) داده برای همیشه و نیز اگر داده‌ای به مصرف رسیده باشد، قطع ارتباط آن داده با محل مصرفش است. دلایلی که برای وارهایی امن داده‌ها وجود دارد ممکن است شامل موارد زیر باشند:

- کاهش ریسک نشت داده،
- حذف داده‌های نامناسب یا نادرست،
- اعمال حق به فراموشی سپردن،
- انطباق با موافقت‌نامه‌های قراردادی با مشتریان یا تأمین‌کنندگان،
- انطباق با الزامات یا مقررات قانونی.

۳-۵- راهنمای حکمرانی داده‌ها - اصول

۳-۵-۱- اصل ۱: مسئولیت

بدنه حکمرانی درباره‌ی مسئولیت‌های مربوط به استفاده‌ی سازمان از داده‌ها پاسخگو است و باید اطمینان حاصل کند که درون سازمان، مسئولیت‌های خود را درک کرده و پذیرفته است. این مسئولیت‌ها شامل موارد زیر می‌شوند:

- در سراسر سازمان و فراتر از عملکرد یا بخش فناوری اطلاعات، یا فعالیت‌های بنیادین فناوری اطلاعات گسترش یابد.
- داده‌های کلیدی مربوط به فعالیت‌های کسب‌وکار مانند بازاریابی را شامل شود که در آن داده‌ها برای اطلاع‌رسانی طرح‌های محصول و توسعه محصول استفاده می‌شود و نیز برای راهنمایی طراحی و ساخت محصولات جدید جمع‌آوری می‌شوند.
- شامل وضعیت‌هایی می‌شود که در آن‌ها خود داده به عنوان محصول یا خدمتی توسط سازمان ارائه می‌شود (مانند اطلاعات آب‌وهوا یا بازار سهام)
- پوشش کل چرخه عمر داده‌ها

۳-۵-۲- اصل ۲: راهبرد (استراتژی)

بدنه‌ی حکمرانی در خصوص همراستایی قابلیت‌های کنونی و آینده راهبرد داده‌ها با راهبرد کلی سازمان پاسخگو است. این راهبردها باید:

- شامل طرح‌هایی برای به کارگیری داده‌ها در راستای اهداف راهبردی کنونی و آینده باشد.
- امکان اعمال پیشرفت‌های فناوری و انتظارات بازار وجود داشته باشد.
- تمام قسمت‌های نقشه پاسخگویی و تعهدپذیری داده‌ها را پوشش دهد.
- به جنبه‌های خاص داده‌های حکمرانی (ارزش، ریسک، محدودیت‌ها) توجه کند.
- امکان بازنگری کلی راهبرد برای پاسخگویی و تعهدپذیری در برابر فرصت‌ها یا مخاطرات جدید وجود داشته باشد.

۳-۵-۳- اصل ۳: دریافت (اکتساب)

بدنه‌ی حکمرانی در خصوص اکتساب داده‌ها (شامل جمع‌آوری یا خرید، یا به عنوان محصول جانبی یک کسب‌وکار) پاسخگو است و باید اطمینان یابد که آیا اکتساب‌های موجود با در نظر گرفتن موارد زیر مناسب هستند یا خیر:

– اکتساب داده با کاربرد مورد نظر و/ یا تعریف شده‌ی آن در درون سازمان و نیز کاربرد خارجی (در صورت توزیع داده‌ها) سازگار است.

– ارزیابی ارزش، مخاطرات و محدودیت‌های مربوط به کاربرد پیشنهادی و مدیریت مجموعه داده‌های به دست آمده یا جریان داده‌ها با راهبرد داده‌ها همراستا است.

۳-۵-۴- اصل ۴: کاربرد (کارایی)[1]

بدنه‌ی حکمرانی باید معیارهای عملکرد مربوطه را شناسایی کند و اطمینان یابد که در صورت نیاز، به آن معیارها توجه کافی می‌شود و اقدامات اصلاحی اعمال می‌شوند. معیارهای عملکردی باید شامل موارد زیر باشند:

– کاربری خوب و مناسب داده‌ها تا چه اندازه مؤید و پشتیبان تصمیم‌گیری‌های سازمان است.

– کاربری خوب و مناسب داده‌هایی که با تأمین‌کنندگان یا مشتریان به اشتراک گذاشته می‌شود، تا چه اندازه مؤید و پشتیبان تصمیم‌گیری‌ها است.

– نرخ پذیرش مجموعه داده‌های جدید و داده‌های در گردش (جاری) در سازمان (به چه میزان است)

– سود سرمایه‌گذاری روی داده‌ها شامل داده‌هایی که توزیع شده‌اند، (چقدر است)

– بهایی که سازمان به ارزش کلی داده‌ها می‌دهد در قیاس با بهایی که سازمان‌های رقیب یا مشابه به ارزش کلی داده‌ها می‌دهند (چقدر است)

۳-۵-۵- اصل ۵: همخوانی[2]

بدنه‌ی حکمرانی باید اطمینان یابد که سازمان تعهدات خارجی را می‌داند، پیروی می‌کند، به درستی تعریف می‌کند، و پیاده‌سازی می‌کند و از انطباق با خط‌مشی‌های داخلی مطمئن است. این تعهدات و خط‌مشی‌ها باید شامل موارد زیر باشند:

– تمامی مجموعه داده‌ها (دیتاست‌ها) و جریان‌های داده مطابق با خط‌مشی‌های امنیتی که نیازها و تعهدات سازمان را برآورده می‌کنند، ایمن شده‌اند.

– ساماندهی صحیح اطلاعات شخصی قابل شناسایی (PII[3])

[1] Performance
[2] Conformance
[3] Personal Identifiable Information

- پیاده‌سازی مناسب خط‌مشی‌ها و شیوه‌های حفظ داده‌ها در سراسر سازمان
- درک تمام تعهدات قانونی مربوط داده‌ها و حصول اطمینان از اینکه این تعهدات در سراسر سازمان برآورده شده‌اند.

۳-۵-۶- اصل ۶: رفتار انسانی[1]

بدنه‌ی حکمرانی در برابر کاربری داده‌ها در سراسر سازمان متعهد و پاسخگو است به طوریکه رفتارهای انسانی به درستی شناسایی و در نظر گرفته شده باشند. چنین ارج‌گذاری به رفتار انسانی باید موارد زیر را در برگیرد:

- خط‌مشی‌ای برای هدایت کاربری پذیرفته شده داده‌ها و افزاره‌ها (تجهیزات) در سراسر سازمان،
- فرهنگ سازمانی در پیوند با داده‌ها باید مشوق اشتراک‌گذاری، حفظ و تفسیر مناسب داده‌ها باشد.
- اثرات و الزامات رفتار انسانی ذینفعان

۳-۶- راهنمایی برای حکمرانی داده‌ها- مدل

۳-۶-۱- به کارگیری مدل

* بدنه‌ی حکمرانی باید داده‌ها را از طریق سه وظیفه اصلی زیر نظارت و مدیریت کند:

الف) ارزیابی کاربرد فعلی و آینده داده‌ها

ب) آماده‌سازی و پیاده‌سازی مستقیم راهبردها و خط‌مشی‌ها برای اطمینان از برآورده شدن اهداف کسب‌وکار با به کارگیری داده‌ها

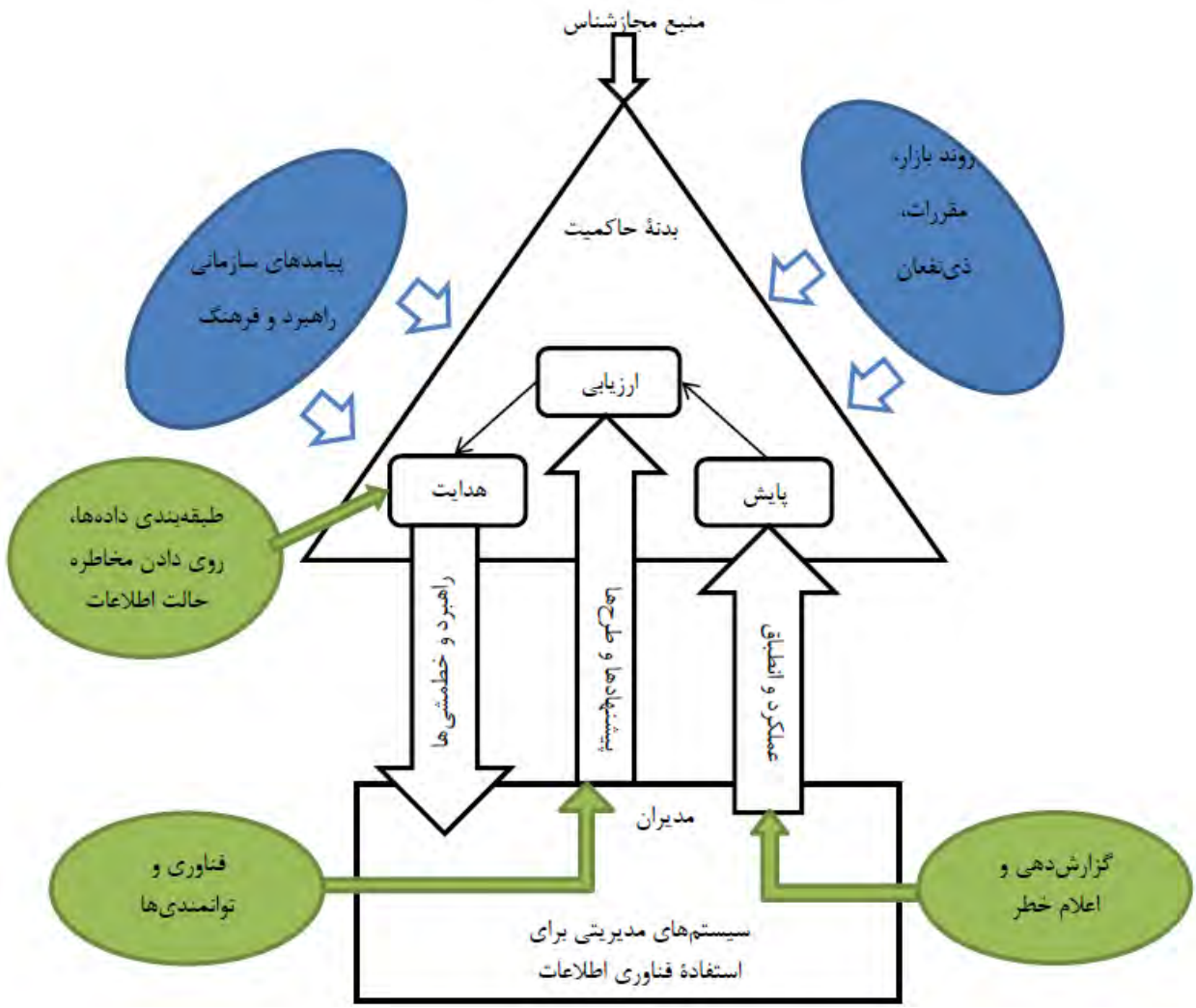
پ) پایش انطباق با خط‌مشی‌ها و عملکرد در برابر راهبردها

* مجازشناسی[2] جنبه‌های خاص فناوری اطلاعات می‌تواند به مدیران درون سازمان تفویض شود، اما پاسخگویی و تعهدپذیری برای استفاده‌ی مؤثر، کارا و قابل قبول فناوری داده‌ها توسط سازمان همچنان با بدنه‌ی حکمرانی است و نمی‌تواند تفویض شود.

شکل ۹، فشارهای خاص وارده بر بدنه‌ی حکمرانی را در رابطه با داده‌ها و استفاده از آن‌ها توسط سازمان نشان می‌دهد. ذینفعان در این شکل شامل مشتریان، کارکنان و تنظیم‌کنندگان مقررات می‌شوند. در این شکل همچنین انواع ورودی‌های[3] مورد

[1] Human behavior
[2] Authority
[3] Inputs

نیاز چرخه EDM که به داده‌ها مربوطند، نشان داده شده است. نواحی که در آن‌ها، ورودی‌های مدیریت می‌تواند در فعالیت‌های هدایت، ارزیابی و پایش به بدنه‌ی حکمرانی کمک کند، در این نمودار نشان داده شده است.



شکل ۹- مدل حکمرانی فناوری اطلاعات- کاربرد آن در حکمرانی داده

۳-۶-۲- الزامات داخلی

– بدنه‌ی حکمرانی باید برای برآوردن تعهدات خود به ذینفعان، استفاده از داده‌ها را به عنوان بخشی از راهبرد کلی بررسی کند.

– لازم است بدنه‌ی حکمرانی، استفاده‌ی بالقوه از داده‌ها را در خود سازمان یا سازمان‌های رقیب بررسی کند و راهبردی برای پشتیبانی از پیامدهای مطلوب جهت‌دهی کند. این عمل ممکن است شامل خرید و فروش داده‌ها باشد.

– بدنه‌ی حکمرانی باید فرهنگ داده‌ای را به گونه‌ای ترسیم کند تا اطمینان یابد که آن فرهنگ با راهبرد داده‌های مورد نیاز برای رسیدن به اهداف کلی بدنه‌ی حکمرانی هم‌راستاست.

۳-۶-۳- فشارهای خارجی

* سازمان ممکن است برای اطمینان از سازگاری با فشارهای بازاری که در آن فعالیت دارد، نیاز به تنظیم راهبردها و خط‌مشی‌هایی داشته باشد. چنین فشارهایی عبارت‌اند از:

– انتظارات مشتری در خصوص وارهایی (از بین بردن)، کیفیت و تعامل با داده‌های موجود

– 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 بدنه‌ی حکمرانی باید اطمینان یابد که راهبردها و خط‌مشی‌ها برای استفاده فعلی و آینده داده‌ها در این بازارها به طور گسترده اعمال شوند. چنین محدودیت‌ها و تعهداتی ممکن است در فعالیت‌های مختلف پاسخگویی و تعهدپذیری داده‌ها اعمال شوند، از جمله:

– چگونگی جمع‌آوری داده‌ها به نحوی که شامل اطلاع‌رسانی‌های (اعلان‌های) حریم خصوصی و الزامات رضایت درباره‌ی جمع‌آوری و استفاده از اطلاعات شخصی شوند.

– الزامات نگهداری و وارهایی داده‌ها

– تعهدات تصمیم‌گیری برای برخورد مناسب با تعصبات، تبعیض و نمایه‌سازی

– مسائل مربوط به مالکیت معنوی درباره‌ی به اشتراک‌گذاری یا بازاستفاده از داده‌ها.

۳-۶-۴- ارزیابی

– در ارزیابی حکمرانی داده برای سازمان، بدنه‌ی حکمرانی باید به الزامات داخلی و فشارهای خارجی وارد بر سازمان توجه کند.

– بدنه‌ی حکمرانی باید استفاده‌ی کنونی و آتی 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 و انتظارات اجتماعی

– عوامل دیگری که استفاده از داده‌ها را واپایش (کنترل) می‌کنند و بر آن تأثیر می‌گذارند.

– بدنه‌ی حکمرانی باید پیشنهادهای مدیران را برای توضیح فناوری‌های (جدید) مدیریت داده‌ها و تأثیر بالقوه آن‌ها بر سازمان درخواست کند (چنین فناوری‌هایی می‌توانند تأثیر قابل توجهی بر هزینه، بینش و حریم خصوصی داشته باشند و در بسیاری از موارد، این اثرات می‌تواند فراتر از مدیریت داده‌ها باشد و فرصت‌های کسب‌وکار جدید و به طور بالقوه ریسک بزرگتری را برای سازمان به همراه آورند)

– بدنه‌ی حکمرانی همچنین باید از توانمندی‌های مدیریت داده‌های سازمان مطلع باشد. برای مثال:

– سازمان تا چه اندازه می‌تواند نقض داده را بهبود بخشد.

– اطلاعات صحیح چگونه به آسانی می‌توانند در قالب درست برای کمک به تصمیم‌گیری در همه سطوح تحویل داده شوند.

– آیا سازمان فناوری‌های جدید مانند رایانش ابری را برای افزایش توانمندی‌های خود به کار می‌گیرد.

۳-۶-۵- هدایت[1]

– بدنه‌ی حکمرانی باید مسئولیت‌پذیری (وظیفه‌ای) را برای آماده‌سازی و پیاده‌سازی مستقیم راهبردها و خط‌مشی‌های (داده) اختصاص دهد.

– راهبردها و خط‌مشی‌های استفاده کنونی و آتی داده‌ها برای سازمان باید در جهت اهداف زیر باشند:

– بیشینه کردن ارزش سرمایه‌گذاری سازمان در داده‌ها

– مدیریت مخاطره مرتبط با داده‌ها با توجه به سطح ریسک‌پذیری آن‌ها (مانند ارزش و ریسک بالای مدیریت داده‌های بازار سهام)

– اطمینان از سطح صحیح نظارت[2] بر داده‌ها: فعالیت‌های پاسخگویی و تعهدپذیری داده‌ها باید به طرز مناسبی درون سازمان تفویض شوند.

[1] Direct
[2] Stewardship

۳-۶-۶- پایش

– بدنه‌ی حکمرانی باید از طریق سیستم‌های اندازه‌گیری مناسب، بهره‌برداری از داده‌های سازمان را پایش کنند. این اطمینان باید حاصل شود که راهبردهای مربوط به داده‌ها به درستی پیاده‌سازی شده‌اند 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 فرآیندهای تصمیم‌گیری اندازه‌گیری شود.

– بخش‌های دیگری که نظارت بدنه‌ی حکمرانی به دلیل راهبردی یا مقرراتی ممکن است از اهمیت زیادی برخوردار باشد، عبارت‌اند از:

– استفاده از PII شامل مسائل مربوط به حفظ حریم خصوصی، الزامات رضایت و شفافیت استفاده از داده‌ها (به استاندارد ISO/IEC 29100 مراجعه شود)

– استفاده از سیستم مؤثر مدیریت امنیت اطلاعات که اهمیت استراتژیک (راهبردی) داده را نشان می‌دهد(استاندارد ISO/IEC 27001 و استاندارد ISO/IEC 27017). در این استانداردهای بین‌المللی دستورالعملی برای واپایش‌های (کنترل‌های) امنیت اطلاعات در برخی موارد ارائه شده است اما چنین واپایش‌هایی کافی نخواهد بود و بدنه‌ی حکمرانی باید به اعتماد و درستی‌سنجی (وارسی) تکیه کند.

– الزامات نگهداری و وارهایی داده‌ها

– بازاستفاده، به اشتراک‌گذاری یا فروش داده‌ها و حقوق مربوط به آن‌ها، صدور مجوز یا حق نشر

– اصول حسابرسی[1] مناسب برای هنجارهای فرهنگی، تعصب، تبعیض یا نمایه‌سازی[2] در تصمیم‌گیری

[1] Accounting
[2] Profiling

۳-۷- راهنمای حکمرانی داده- جنبه‌های خاص داده

۳-۷-۱- ارزش

داده‌ها می‌توانند به عنوان یک ماده خام برای کسب اطلاعات مفید توزیع شوند و به فروش روند. برای استخراج اطلاعات از داده‌ها لازم است تا داده‌ها دارای *کیفیت*، *بهنگام بودن*، *متن (محتوا)*[1]، حجم و به طور بالقوه ویژگی‌های دیگری برای مطابقت با الزامات فرآیندهای تصمیم‌گیری باشند.

۳-۷-۲- ریسک (مخاطره)

از آن‌جایی که داده‌ها دارای ارزش هستند با ریسک نیز همراه هستند. یک راه برای کاهش ریسک سازمان در استفاده از داده‌هایی مانند داده‌های مراقبت‌های بهداشتی، حذف ویژگی‌های PII از طریق فنون هویت‌زدایی (شناسایی‌ناپذیری)[2] شرح داده شده در استاندارد ISO/IEC 20889 است.

-ریسک‌های مربوط به داده‌ها باید توسط بدنه‌ی حکمرانی بررسی شوند تا اطمینان حاصل شود که سطح مناسبی از ریسک داده تنظیم شده است که با ریسک کلی هم‌راستاست.

- همچنین ریسک عدم استفاده از داده‌های موجود برای منافع سازمان نیز باید در نظر گرفته شوند. به بیان دیگر اگر مشخص شود چنین داده‌هایی موجود هستند اما براساس آن‌ها عمل نمی‌شود نیز ممکن است به ضرر سازمان باشد. 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 منجر شود.

۳-۷-۲-۱- مدیریت

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

[1] Context
[2] De-identification

برای تغییر فرآیندهای مدیریت ریسک به منظور در نظرگرفتن ریسک داده‌ها (یا هر تغییری در نمایه ریسک یا ریسک‌پذیری)، در زیربند ۳-۲ استاندارد ISO/TR 31004:2013 توصیه شده است که: سازمان باید تغییراتی را که برای چارچوب مدیریت ریسک لازم است، قبل از برنامه‌ریزی و پیاده‌سازی آن تغییرات و پایش مداوم اثربخشی چارچوب اصلاح شده تعیین کند.

۳-۷-۲-۲- طرح‌های طبقه‌بندی (کلاس‌بندی) داده‌ها[1]

- بدنه‌ی حکمرانی باید منابعی را برای به کارگیری و حفاظت داده‌ها با تأکید بر ارزش بالا و ریسک بالای داده‌ها اختصاص دهد.

- به عنوان بخشی از یک سیستم مدیریت امنیت اطلاعات (ISMS)، مدیران باید انواع مختلف داده‌ها را از طریق طرح طبقه‌بندی داده‌ها شناسایی کنند. چنین طرحی به سازمان اجازه می‌دهد تا سطوح مختلف منابع را برای انواع(طبقه‌های) مختلف داده‌ها به کار گیرند. در زیربند ۸-۲-۱ استاندارد ISO/IEC 27002:2013 بیان شده است که: اطلاعات باید برحسب الزامات قانونی، ارزش، حیاتی بودن و حساسیت به افشا یا تغییر غیرمجاز طبقه‌بندی شوند.

۳-۷-۲-۳- امنیت

* امنیت، عنصری از مدیریت ریسک است. بدنه‌ی حکمرانی باید نظارت قوی بر امنیت داده‌ها در چارچوب امنیت سازمان داشته باشند.

* هنگام ارزیابی راهبردها و خط‌مشی‌های تأیید شده برای امنیت داده‌ها، می‌توان معیارهای حفاظتی زیر را در نظر گرفت:

- چارچوب امنیت IT مانند «چارچوبی برای بهبود امنیت سایبری زیرساخت حیاتی » از NIST از برنامه‌های راه‌انداز کسب‌وکار به منظور هدایت فعالیت‌های امنیت سایبری به عنوان بخشی از چارچوب مدیریت مخاطرات استفاده می‌کند
- ISMS مانند مجموعه استانداردهای ISO/IEC 27000 که شامل واپایش‌ها(کنترل‌ها)ی امنیتی خاص است.
- در مواردی که PII توسط ارائه‌دهنده خدمات ابری پردازش می‌شود، استاندارد ISO/IEC 27018 واپایش‌هایی را به منظور اطمینان از حفاظت داده‌ها تعیین کرده است.

۳-۷-۳- محدودیت‌ها (تنگناها)

- مقررات و قوانین: مقررات و قوانینی مانند قوانین متداول و قوانین قراردادی ممکن است بر دسترسی، استفاده، ذخیره یا توزیع داده‌ها اعمال شوند و باید در فرمول‌بندی راهبردها و خط‌مشی‌های داده‌ها بدان توجه کرد.

[1] Data classification schemes

– جامعه‌نگر (جامعه‌ای)[1]: از دیدگاه راهبردی این جنبه به قرارداد ضمنی[2] با جامعه مربوط است (برای مثال اهدف اصلی خدمات بهداشت عمومی می‌تواند حفظ سلامت کل جامعه و نه سلامت فردی باشد). بدنه‌ی حکمرانی می‌تواند درباره‌ی قرارداد ضمنی به شفاف‌سازی راهبرد داده‌ها مانند چگونگی استفاده از داده‌ها و تصمیم‌گیری به وسیله داده‌ها کمک کند.

۳-۷-۳-۱- خط مشی سازمانی

سازمان ممکن است خط‌مشی خود را بر روی داده‌ها برای افزایش ارزش آن‌ها، کاهش هزینه‌های مدیریت داده‌ها، کاهش مخاطرات مربوط به داده‌ها یا برای برآوردن الزامات دیگر اعمال کند.

۳-۸- به کارگیری نقشه تعهدپذیری داده‌ها

اعمال اصول حکمرانی IT طبق استاندارد ISO/IEC 38500، چارچوب حکمرانی IT 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.

براین اساس، با تلفیق نقشه پاسخگویی و تعهدپذیری داده‌ها با جنبه‌های گوناگون داده‌ها همچون ارزش، ریسک و محدودیت‌ها، راهنمایی برای یک چک‌لیست جامع ملاحظات برای بدنه‌ی حکمرانی فراهم می‌شود (این چک‌لیست راهنمای ایجاد چارچوب حکمرانی را برای بدنه‌ی حکمرانی فراهم می‌کند)

– بدنه‌ی حکمرانی باید از جدول ۱ به عنوان راهنمایی برای ارزیابی، پایش و هدایت فعالیت‌های سازمانی برای حکمرانی داده به طور کلی و برای رده‌های خاص داده‌ها– اگر مناسب باشد– استفاده کند. برای هر فعالیت پاسخگویی و تعهدپذیری داده‌ها، باید جنبه‌های خاص داده‌ها را بررسی کرد تا مشخص شود که آیا اقداماتی با سطوح بالاتر واپایش و خط‌مشی سختگیرانه‌تر برای جمع‌آوری داده‌هایی باارزش بیشتر یا حساسیت بیشتر نیاز خواهد بود.

چک‌لیست ارائه شده فراگیر نیست و بدنه‌ی حکمرانی باید موقعیت خود را ارزیابی کند و در صورت لزوم، اقدامات افزون‌تری را انجام دهد.

[1] Societal
[2] Implied contract

جدول ۱- نواحی داده‌ها و جنبه‌های خاص داده‌های حکمرانی (یک چک‌لیست نمونه خلاصه شده)

	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 یا 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 تعهدپذیری 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.

۴- استاندارد ISO/IEC TR 38505-2: فناوری اطلاعات-حکمرانی IT- حکمرانی داده: بخش۲: پیاده‌سازی ISO/IEC 38505-1 برای مدیریت داده

۴-۱- هدف و دامنه‌ی کاربرد

هدف از تدوین استاندارد ISO/IEC TR 38505-2 ارائه اصول راهنما برای اعضای بدنه‌ی حکمرانی سازمان‌ها و مدیران اجرایی آن‌ها به منظور پیاده‌سازی استاندارد ISO/IEC 38505-1 برای مدیریت داده است. در این جا فرض می‌شود که درک کاملی از مفاهیم و اصول معرفی شده در استاندارد ISO/IEC 38500 وجود دارد و خواننده با نقشه تعهدپذیری و پاسخگویی داده‌ها و ملاحظات معرفی شده در استاندارد ISO/IEC 38505-1 آشنایی دارد. در این سند موضوعات زیر پوشش داده می‌شود:

- شناسایی اطلاعاتی که نهاد حکمرانیی برای ارزیابی و هداف راهبردها (استراتژی‌ها) و خطمشی‌های (سیاست‌های) مرتبط به کسب‌وکارهای مبتنی بر داده‌ها به آن‌ها نیاز دارد.

– شناسایی قابلیت‌ها و پتانسیل‌های سیستم‌های اندازه‌گیری که می‌توانند برای پایش (نظارت) بر عملکرد داده‌ها و کاربردهای آن مورد استفاده قرار گیرند.

۴-۲- نقش‌های مدیریتی و حکمرانی

۴-۲-۱- نقش حکمرانی

صرف‌نظر از اینکه بدنه حکمرانی چه راهبرد یا ریسک‌پذیری را برای حکمرانی داده اتخاذ کند، بدنه‌ی (نهاد) حکمرانی همچنان در قبال داده‌ها و کاربرد آن‌ها توسط سازمان (شامل تمام تصمیمات نشأت گرفته از داده‌ها یا مرتبط با داده‌ها در سازمان) متعهد و پاسخگو باقی می‌ماند.

در استاندارد ISO/IEC 38505-1 نگاشتی از نقشه تعهدپذیری و پاسخگویی داده به حوزه‌های ارزیابی داده شامل ارزش، ریسک و محدودیت‌ها ارائه شده است که به شناسایی مسائل و موضوعات و در نتیجه تعریف خط‌مشی‌های مورد نیاز برای پیاده‌سازی راهبرد کلی سازمان کمک می‌کند (چک‌لیست ارائه شده در این استاندارد کامل نیست و سازمان‌ها برحسب شرایط سازمانی خود اقدامات دیگری را به آن اضافه می‌کنند.) مفاهیم چک‌لیست ارائه شده در استاندارد ISO/IEC 38505-1 می‌تواند برای توصیف خط‌مشی‌ها و راهبردهایی که باید پیاده‌سازی شوند، مورد استفاده قرار گیرند. این چک‌لیست به عنوان مرجعی در سند پیش‌رو استفاده می‌شود.

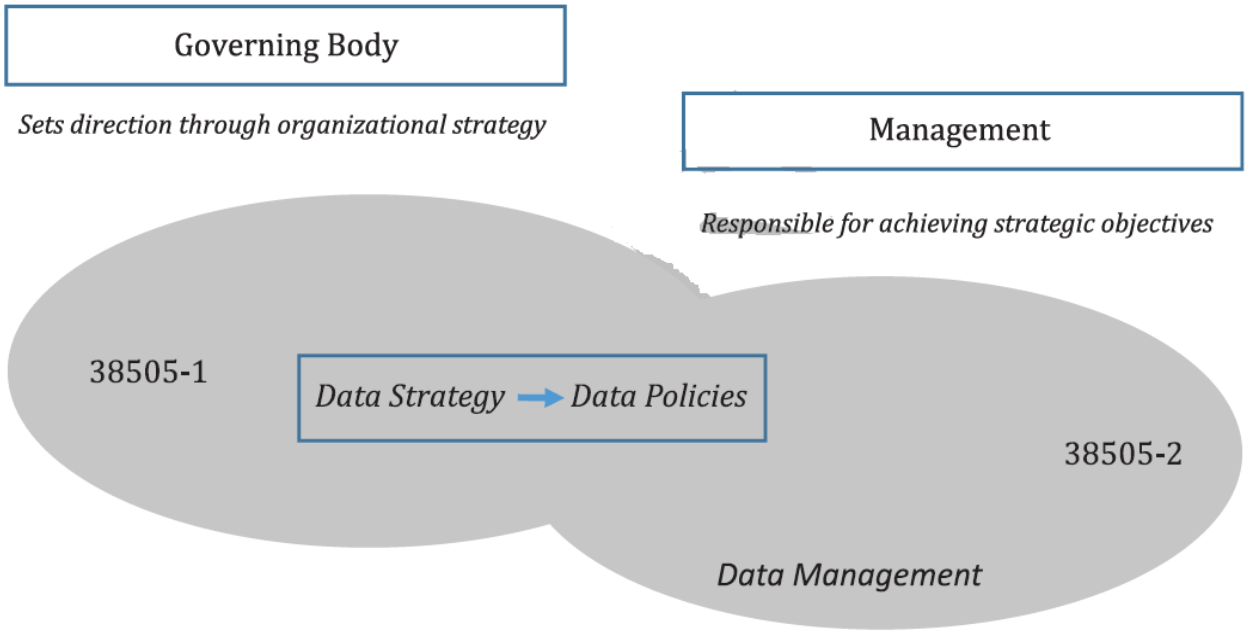
۴-۲-۲- نقش مدیریت

– در مورد داده‌ها (که بدنه‌ی حکمرانی ممکن است–می‌تواند– از توانایی‌های مسئولین مدیریت داده‌ها بی‌اطلاع باشد) نه بدنه‌ی حکمرانی و نه تیم مدیریتی نباید به طور جدا از طرف مقابل (به طور جداگانه) خط‌مشی تعیین کنند (انتظار می‌رود که این کار را انجام ندهند).

– تیم مدیریتی و بدنه‌ی حکمرانی باید (انتظار می‌رود) در مورد قابلیت (توانایی) فعلی و مطلوب آینده‌ی سازمان برای مدیریت داده‌ها توافق کنند. بهره‌گیری از بازارها یا محصولات جدیدی که از جمع‌آوری و استفاده دقیق از داده‌ها حاصل می‌شوند نیز می‌تواند سودمند باشد.

در شکل ۱۰ به صورت شماتیکی نشان داده شده است که بدنه‌ی حکمرانی مسئول تعیین راهبردها(استراتژی‌ها) و خط‌مشی‌های داده برای سازمان و اطمینان از همسویی آن‌ها با راهبرد کلی سازمان است. این تیم مدیریتی است که در چارچوب اختیارات

تفویض شده خود، مسئول اجرای این خطمشی‌ها است. در این شکل، جزئیات رابطه بین بدنه‌ی حکمرانی و تیم مدیریت نشان داده نشده است (مانند اینکه چگونه آن‌ها برای تدوین استراتژی‌های سازمانی با در نظر گرفتن محدودیت‌ها و ملاحظات ذینفعان با یکدیگر همکاری می‌کنند). عنصر مهم دیگری که در این شکل نشان داده نشده است، تأثیر فرهنگ سازمان[1] و چگونگی نفوذ آن در تمام جنبه‌های تعهدپذیری (پاسخگویی) و پیاده‌سازی راهبرد است.



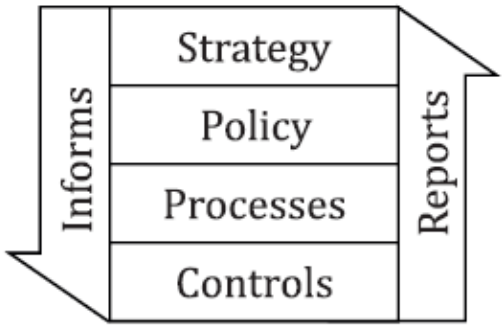
شکل ۱۰- راهبرد و خطمشی‌های داده

در این سند و در ادامه نشان داده می‌شود که چگونه می‌توان از چک لیست ملاحظات استاندارد ISO/IEC 38505 (ملاحظات توسعه چارچوب حکمرانی داده) برای ایجاد خطمشی‌های داده استفاده کرد.

۴-۳- ارتباط راهبرد(استراتژی) کسب‌وکار با مدیریت داده

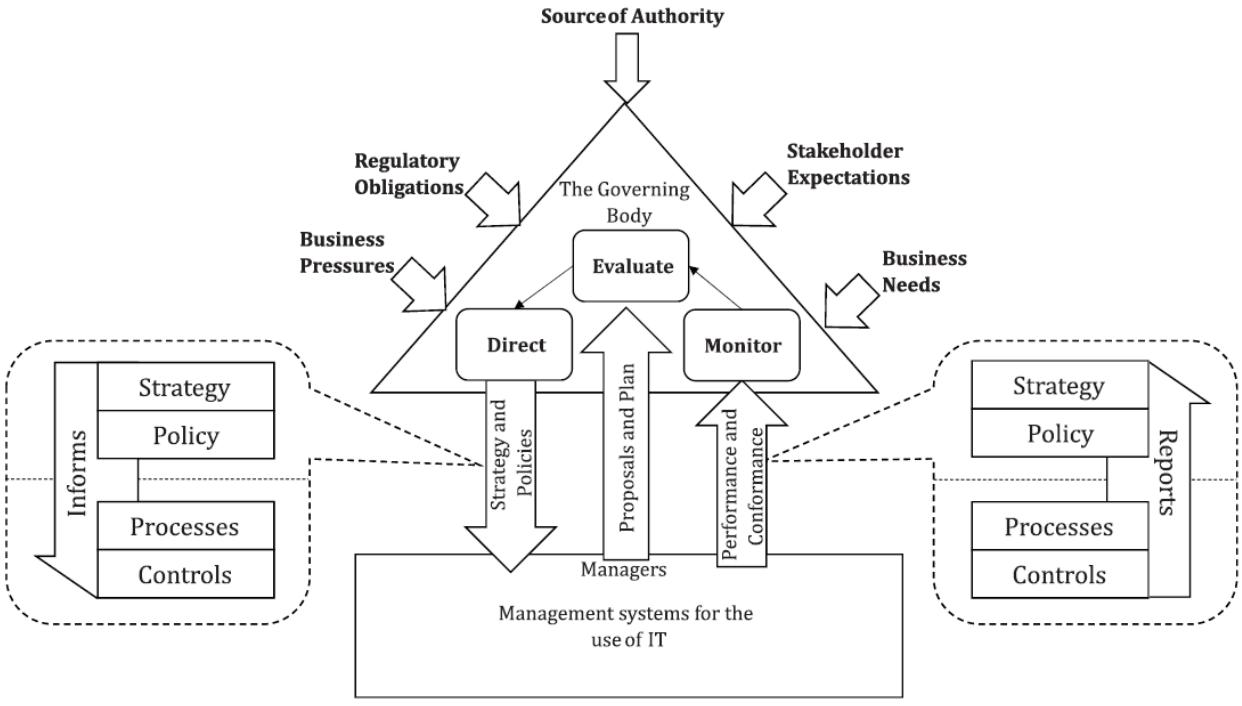
در این بند، نحوه پیاده‌سازی راهبرد کسب‌وکار از طریق توسعه خطمشی، فرآیندها و کنترل‌ها توضیح داده می‌شود. تمرکز این سند بر توسعه خطمشی از طریق مشارکت اعضای بدنه‌ی حکمرانی با اعضای تیم مدیریت است.

[1] Culture of the organization



شکل ۱۱- سازوکار سری (متوالی) [1]

در شکل ۱۱، راهبرد توسط بدنه‌ی حکمرانی توسعه می‌یابد و بیانگرخط‌مشی (خط‌مشی توسط بدنه‌ی حکمرانی و با مباحثه با تیم مدیریت تدوین می‌شود) است و به نوبه‌ی خود راهنمایی برای توسعه فرآیندهای مناسب محسوب می‌شود. کنترل‌ها (واپاشی‌ها) نیز امکان تطابق فرآیندها با راهبرد را میسر می‌سازند. توجه کنید که توالی نشان داده شده یک ارتباط دوطرفه است و باید اطمینان حاصل شودکه سازوکار بازخوردی از کنترل‌ها به سمت استراتژی وجود دارد. بدنه‌ی حکمرانی می‌تواند از طریق دریافت گزارشات وهشدارهای تولید شده توسط کنترل‌ها، عملکرد و انطباق را پایش کند و از همسویی راهبرد تا اجرا اطمینان یابد.



شکل ۱۲- ارتباط حکمرانی داده با مدیریت داده

[1] Cascade mechanism

در شکل ۱۲ نشان داده شده است که چگونه بدنه‌ی حکمرانی و تیم‌های مدیریتی برای اجرای خط‌مشی و حمایت از راهبردی سازمانی و به طور خاص راهبرد داده‌ها با یکدیگر همکاری می‌کنند. همان‌طور که بیان شد، بدنه (نهادهای) حکمرانی و مدیریتی از طریق سازوکار متوالی (cascade) که شامل عناصر راهبرد، خط‌مشی، فرآیندها و کنترل‌ها (واپایش‌ها) می‌شود با یکدیگر در ارتباط هستند. این اتصالات از طریق مدل EDM به شرح زیر توسعه داده و نگهداری می‌شوند:

ارزیابی (Evaluate): طراحی پیشنهادها و برنامه‌هایی اجرایی و همچنین ارزیابی فعالیت‌ها به منظور تحقق راهبرد سازمانی تدوین شده توسط بدنه‌ی حکمرانی (هیئت حاکمه) برعهده بدنه‌ی مدیریتی است. در طرح‌ها و پیشنهادات باید(انتظار می‌رود)[1] معرفی فناوری‌های نوین مانند فناوری کلان داده که منجر به بهبود کاربرد داده‌ها می‌شوند، در نظر گرفته شوند. همچنین قابلیت‌های فعلی و آتی زیرساخت‌های اساسی (حیاتی) برای انجام فعالیت‌های مدیریت داده باید (انتظار می‌رود) در نظر گرفته شوند. فناوری و قابلیت‌ها (توانایی‌ها) باید در فرآیندهای مدیریتی که بیانگر فعالیت‌های مدیریتی هستند، توضیح داده شوند. بدنه‌ی حکمرانی با به کارگیری پیشنهادات و برنامه‌های مدیریتی در کنار سایر منابع اطلاعاتی قادر به ارزیابی راهبرد داده مناسب خواهد بود.

هدایت (Direct): بدنه‌ی حکمرانی راهبردها و خط‌مشی‌های داده برای حکمرانی داده را تدوین می‌کند و مسئولیت‌ها و تعهدپذیری‌ها (پاسخگویی‌ها) را برای ایجاد ساختار حکمرانی تعیین می‌کند. بدنه‌ی حکمرانی توسعه راهبرد و خط‌مشی‌های داده را مطابق جنبه‌های نقشه تعهدپذیری و پاسخگویی که در استاندارد ISO/IEC 38505-1 معرفی شده است، هدایت می‌کند. فعالیت‌هایی که باید در نظر گرفته شوند شامل طبقه‌بندی (کلاس‌بندی) داده‌ها و ریسک‌پذیری سازمان در رابطه با داده‌ها است. این نگاشت به توسعه خط‌مشی برای مدیران (تا آن‌ها را با در نظر گرفتن جنبه‌های ارزش، ریسک و محدودیت‌ها اجرا کنند) کمک می‌کند.

پایش (Monitor): بدنه (نهاد) حکمرانی باید بر عملکرد و انطباق فعالیت‌های مدیریتی نسبت به جهت‌های تعیین شده نظارت کند. گزارش‌ها و هشدارهای ارائه شده توسط بدنه‌ی مدیریت در انجام این وظیفه کمک خواهند کرد. این گزارش‌ها باید(انتظار می‌رود) شامل گزارشات وضعیت مربوط به همسویی با قوانین و مقررات و اطلاع‌رسانی در مورد وقوع رویدادهای مشخص با ریسک بالا باشند. هشدارها باید هنگام وقوع رویدادهای امنیتی و حریم خصوصی و با ریسک مهم که در فرآیندهای نگاشت (نقشه‌برداری) شناسایی شده‌اند، فعال شوند.

[1] Should

استراتژی داده (راهبرد داده) عمدتاً با محدودیت‌های محیطی و فرصت‌های دستیابی به اهداف و مقاصد سازمانی سروکار دارد، اما خط‌مشی‌داده به مجموعه قوانینی اشاره دارد که توسط سازمان برای تصمیم‌گیری منطقی وضع می‌شود. حکمرانی خط‌مشی داده[1] تدوین شده توسط نهاد حکمرانی باید:

- هماهنگ با راهبرد و اهداف و مقاصد سازمانی باشد.
- با سایر خط‌مشی‌های سازمانی سازگار باشد.
- شامل سازوکارهایی برای اجرای خط‌مشی و بازنگری باشد.

توسعه سیاست در چارچوب حکمرانی داده یک فرآیند مداوم است، بنابراین بدنه‌ی حکمرانی باید اطمینان حاصل کند که وظایف زیر توسط مدیریت انجام می‌شود:

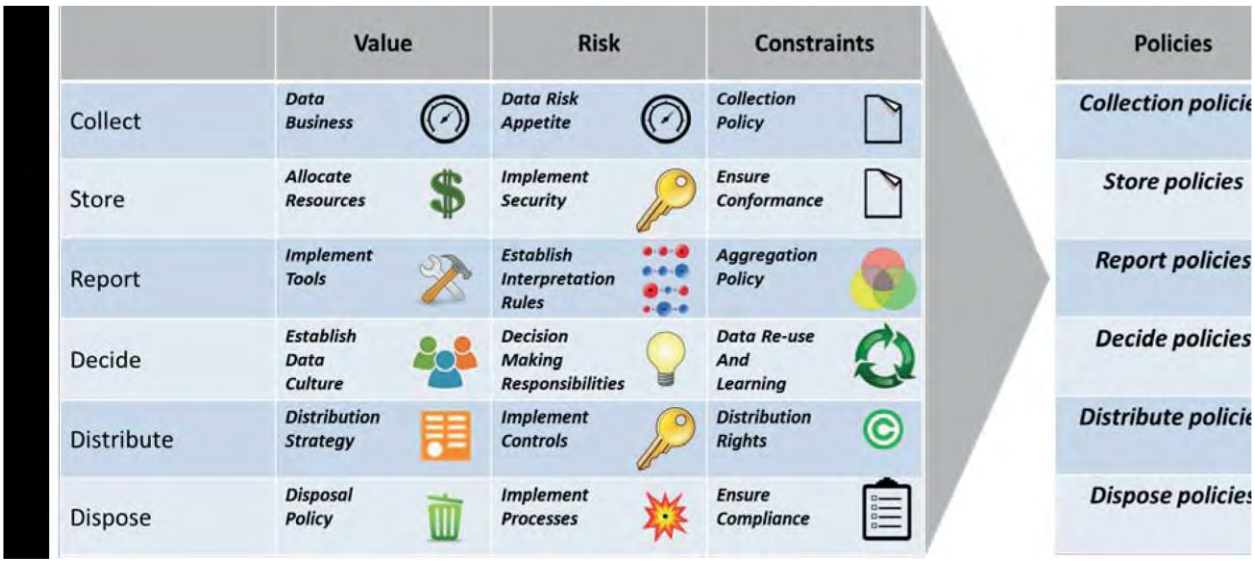
- شناسایی و تعریف:
  - شناسایی الزامات رگولاتوری جدید، پیشرفت‌های فناوری، نیازهای عملیاتی و مسائل و شکاف‌های موجود
  - شناسایی حامیان مالی، ذینفعان و تعیین نقش‌های مرتبط آن‌ها
  - شناسایی فعالیت‌های مختلف تجاری (کسب‌وکار)
  - تدوین روشی برای تعریف خط‌مشی‌ها
  - دریافت تأییدیه برای ادامه پیش‌نویس خط‌مشی
- توسعه:
  - توسعه و پیش‌نویس مجموعه اولیه از خط‌مشی‌ها
  - توزیع پیش‌نویس خط‌مشی بین ذینفعان برای بررسی و اعلام نظر
  - بازبینی و در صورت لزوم، اعمال بازخوردهای دریافتی
  - اخذ تاییدیه[2]
- پیاده‌سازی و نگهداری:
  - ثبت (post) و اعلام خط‌مشی
  - هدایت فعالیت‌های آموزشی و ارتباطی
  - هماهنگی و پشتیبانی از عملیات خط‌مشی

[1] Governance ofdata policy
[2] Approval

- پایش (نظارت) و بهبود
- مستندسازی نتایج و اثرات عملیات
- نظارت بر انطباق و اثربخشی خط‌مشی اجرا شده
- مرور و بررسی اصلاحات در یک چرخه بازنگری سالانه
- طراحی یک فرآیند بهبود مستمر برای مجموعه خط‌مشی‌ها

۴-۴- تعیین خط‌مشی‌ها از طریق چک‌لیست ملاحظات

در این بخش نشان داده می‌شود که نقشه تعهدپذیری داده‌ها و ماتریس ملاحظات مربوطه از استاندارد ISO/IEC 38505-1 چگونه می‌تواند برای کمک به توسعه خط‌مشی سازمانی که با راهبرد داده سازمان هماهنگ است، اعمال شود. در این نقشه ۶ حوزه تمرکز فعالیت‌های حکمرانی و در نتیجه ۶ حوزه مشخص اعمال خط‌مشی ارائه شده است.



شکل ۱۳- طرح مدیریت داده برای استخراج خط‌مشی

در پیوست این سند مثال‌هایی از چگونگی اعمال ماتریس نواحی و ملاحظات ارائه شده است و نوع و محدوده بیانیه‌های خط‌مشی را نشان می‌دهد که می‌تواند از طریق پرسش پیرامون هر سلول ماتریس حاصل شود. مثال‌ها نشان می‌دهند که چگونه این بیانیه‌های خط‌مشی را می‌توان به خط‌مشی‌های سازمانی موجود اضافه کرد یا به صورت خط‌مشی‌های جداگانه‌ای استفاده نمود. در ادامه یک نمونه معرفی شده در این استاندارد تشریح می‌شود.

۴-۵- کاربرگ های نمونه

در جداول زیر، مجموعه‌ای از کاربرگ‌های نمونه[1] برای تنظیم خط‌مشی‌ها و درک استانداردها و راهنمایی‌های موجود ارائه شده است. در هر جدول، برای هریک از ملاحظات ارائه شده در ISO 38505-1، راهنمایی برای تنظیم خط‌مشی مناسب، برخی از گزینه‌های مدیریت داده، پیشنهادهایی برای نظارت بر عملکرد و انطباق و همچنین استانداردها و راهنمایی‌هایی برای کمک به اجرای سیاست آورده شده است. لازم به ذکر است که مثال‌های ارائه شده جامع نیستند و انتظار می‌رود سازمان‌ها ضمن استفاده از این کاربرگ‌ها، آن‌ها را در صورت نیاز برای سازمان خود گسترش دهند.

توضیح: کدهای «V1، R1، C1» و غیره نشان‌دهنده « ارزش ردیف۱، ریسک ردیف۱، محدودیت‌ها ردیف۱» هستند و فقط برای ساده‌سازی نمایش به کار رفته‌اند.

جدول ۲- جمع‌آوری (Collect)

ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)	
V1	**بدنه حکمرانی باید تصمیم بگیرد که سازمان تا چه میزان از داده‌ها در راستای دستیابی به اهداف استراتژیک خود استفاده یا درآمدزایی کند.**	**R1**	**بدنه حکمرانی باید مخاطرات مربوط به جمع‌آوری و استفاده از داده‌ها را بشناسد و با سطح قابل قبولی از ریسک داده‌ها مطابق چارچوب ریسک‌پذیری سازمان موافقت کند. این باید شامل بررسی مخاطرات ناشی از عدم جمع‌آوری و استفاده از داده‌ها نیز می‌شود.**	**C1**	**بدنه حکمرانی باید سیاست‌های جمع‌آوری داده‌ها را با در نظر گرفتن محدودیت‌هایی مانند کیفیت، حریم خصوصی، الزامات رضایت و شفافیت استفاده تأیید کند.**
تمرکز سیاست (خط‌مشی)	*درجه "کسب و کار داده" بودن.* ** استفاده از داده ها از این هدف پشتیبانی می کند* به عنوان مثال: تمرکز ما همیشه بر ارائه محصولی است که انتظارات مشتری از جمله کیفیت، به موقع بودن و قابلیت اطمینان خدمات را برآورده کند.		*سطح قابل قبول ریسک داده.* ** بدنه حکمرانی میزان ریسکی را که سازمان برای دستیابی به اهداف استراتژیک آماده پذیرش آن است، تعیین می‌کند.* به عنوان مثال: ما فقط داده‌های جزئی مانند داده‌های مکان یا آدرس را از مشتریان پرداخت‌کننده خود جمع‌آوری می‌کنیم		*V1 + R1.* ** با استفاده از موازنه ارزش/ریسک، بدنه حکمرانی مرزهایی را برای استفاده از داده‌ها تعیین می کند.* به عنوان مثال: خط‌مشی شرکت دربرگیرنده مقررات بازارهای منطقه‌ای خواهد بود و در آن مناطق، سختگیرانه‌ترین الزامات اتخاذ خواهند شد (مثلاً در اروپای غربی، قانون آلمان را پیش فرض

[1] Example worksheets

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)	
					می‌گیریم[1]، مگر اینکه خلاف آن ذکر شود)	
گزینه‌های مدیریت داده‌ها	راه های جمع آوری داده‌های با ارزش: – خرید/ ایجاد اشتراک داده‌ها – جمع‌آوری کلان داده‌ها – اینترنت اشیا/ حسگرها – فیدهای داده (داده‌یابی) "زمان واقعی" (RSS، OData...)		مخاطرات جمع‌آوری داده و ملاحظات مدیریت مخاطره: – کیفیت داده‌های جمع‌آوری شده – ابعاد مختلف کیفیت داده از جمله کامل بودن، سازگاری، منحصر به فرد بودن، اعتبار و دقت – تأیید ورودی – اجتناب از اسکریپت‌های ورودی – حملات Man-in-the-middle – اعتبار سنجی آدرس – تشخیص تقلب[2]		ملاحظات مدیریت محدودیت‌های جمع‌آوری داده‌ها: – حریم خصوصی_ اعلام اطلاعیه و دریافت رضایت – استفاده از داده‌ها و شفافیت – یکپارچه‌سازی و به روزرسانی اطلاعات شخصی – اجرای سیاست از طریق ارسال نامه/ ایمیل[3]	
نظارت بر عملکرد و انطباق	اطمینان از جمع‌آوری داده‌های ارزشمند: – ثبت مجموعه داده‌هایی که برای تصمیم‌گیری استفاده می‌شوند – ثبت تصمیمات مبتنی بر داده – طبقه‌بندی داده‌ها		اطمینان از مدیریت ریسک داده: – تعیین مسئولیت‌ها برای مصوبات – تعیین فرآیند جمع‌آوری برای مصوبات		اطمینان از مدیریت محدودیت‌های داده: – تخصیص منابع جمع‌آوری – تهیه فهرستی از مقررات و قوانین	
استانداردهای مرتبط			*ISO 31000، در مورد اصول و دستورالعمل‌های مدیریت ریسک؛ *ISO TS 8000، در مورد کیفیت داده‌ها؛ *ISO TR 31004، در مورد راهنمایی برای مدیریت ریسک		*ISO/IEC 29100، در مورد چارچوب حریم خصوصی؛ *ISO/IEC 19944، در مورد جریان داده، دسته‌بندی داده‌ها و استفاده از داده‌ها	

[1] Default to
[2] Fraud detection
[3] Policy enforcement in email

جدول ۳- ذخیره‌سازی (Store)

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)	
V2	**بدنه حکمرانی باید سیاست‌هایی را به منظور تخصیص منابع مناسب برای ذخیره‌سازی و اشتراک داده‌ها تصویب کند به نحوی که امکان استخراج ارزش بالقوه داده‌ها فراهم شود.**	**R2**	**بدنه حکمرانی باید مدیران را به نحوی هدایت کند که اطمینان حاصل شود یک ISMS قابل توسعه به فراهم‌آورندگان داده و فناوری، با منابع، کنترل‌ها و اعتماد کافی وجود دارد که از سطح ریسک‌پذیری تعیین شده فراتر نرود.**	**C2**	**بدنه حکمرانی باید مدیران را به نحوی هدایت کند که اطمینان حاصل شود شیوه‌های ذخیره‌سازی داده‌ها (شامل اشتراک داده‌های شخص ثالث) از محدودیت‌های جمع‌آوری داده‌ها پشتیبانی می‌کند.**
تمرکز سیاست (خط‌مشی)	*تخصیص منابع.* به عنوان مثال: ضروری است که بدانیم سازمان از چه داده‌هایی استفاده می‌کند. بنابراین، خدمات ذخیره‌سازی و اشتراک داده ها باید توسط بخش فناوری اطلاعات تأیید شود (اما نه لزوماً مدیریت شود).		*تعیین کنترل‌های کافی و سطوح اعتماد بر اساس V2 + R1 + V1.* به عنوان مثال: سازمان ما دارای گواهینامه ۲۷۰۰۱ است و این گواهینامه باید حفظ شود.		*V2 + R2 + C1.* به عنوان مثال: داده‌های شناسایی شده مشتری[1] باید در ناحیه مشتری ذخیره شوند. داده‌های گمنام را می‌توان در دفتر مرکزی شرکت ذخیره کرد.
گزینه‌های مدیریت داده‌ها	*ارزش فضای ذخیره‌سازی:* – پردازش ابری – ایجاد اشتراک داده‌ها – مجازی‌سازی (سرورها، دیسک‌ها، شبکه‌ها)		*ISMS* – استانداردهای سری ISO/ IEC 27000 – چارچوب امنیت سایبری NIST – مدیریت رخدادهای امنیتی *مدیریت ریسک رایانش ابری* – قراردادهای سطح خدمات – قابلیت جابه‌جایی[2] و همکاری – جریان داده‌ها و بیانیه‌های کاربرد		*محدودیت‌ها و فراداده‌ها* – فراداده برای محدودیت‌ها، اطمینان از نگهداشت محدودیت‌های داده
نظارت بر عملکرد و انطباق	*اطمینان از تخصیص منابع ذخیره‌سازی مناسب برای داده‌ها:* – منابع ذخیره‌سازی برای ذخیره داده‌ها آماده است.		*اطمینان از ذخیره امن داده‌های ارزشمند و حساس:* – اطمینان از اینکه سیاست امنیت داده‌ها اجرا شده است.		*حصول اطمینان از ذخیره داده‌ها مطابق با سیاست داخلی و حوزه‌های قانونی و نظارتی:*

[1] Customer identified data
[2] Portability

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
					– تهیه گزارش ارزیابی در خصوص ذخیره‌سازی داده‌ها
استانداردهای مرتبط	*ISO/IEC 17788، در مورد بررسی اجمالی و واژگان رایانش ابری؛ *ISO/IEC 17789، در مورد معماری مرجع برای رایانش ابری؛ *ISO/IEC 19941، در مورد قابلیت همکاری و قابلیت انتقال. *ISO/IEC 20000، در مورد مدیریت خدمات		*ISO/IEC 27000، در مورد سیستم‌های مدیریت امنیت اطلاعات؛ *ISO/IEC 27002، در مورد کنترل‌های امنیت اطلاعات؛ *ISO/IEC 27017، در مورد خدمات ابری؛ *ISO/IEC 27035-1، در مورد مدیریت حوادث امنیتی؛ *ISO/IEC 19086، در مورد SLA رایانش ابری		*ISO/IEC 27018، در مورد پردازش PII

جدول ۴- گزارش (Report)

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
V3	**بدنه حکمرانی باید مدیران را به استفاده از ابزارها و فناوری‌های لازم اجبار کند تا اطمینان حاصل شود که ارزش کامل داده‌ها قابل استخراج است.**	**R3**	**بدنه حکمرانی باید اهمیت ماهیت داده‌ها[1]، از جمله هنجارهای فرهنگی و تفسیر نادرست احتمالی آن‌ها را مشخص کند.**	**C3**	**بدنه حکمرانی باید اهمیت رابطه بین داده‌ها و محدودیت‌های آن را مشخص کند، به ویژه اگر داده ها از دیتاست‌های مختلف جمع‌آوری شده باشند.**
تمرکز سیاست (خط‌مشی)	*V1+V2* به عنوان مثال: ابزارهای گزارش‌دهی (یعنی ابزارهایی که داده‌های مرتبط را برای تصمیم‌گیری استخراج می‌کنند) باید در دسترس همه کارکنان باشد و با نیازهای تصمیم‌گیری آنها مطابقت داشته باشد.		*اهمیت ماهیت داده‌ها* به عنوان مثال: کاهش قیمت محصول باید برای همه مشتریان در یک منطقه اعمال شود. استثناهایی مانند فروش حجمی در این سیاست باید توسط بخش بازاریابی تایید شود		*V1 + R1 + C1 و اهمیت محدودیت‌ها و محدودیت‌های جدید در مجموع.* به عنوان مثال: دسترسی به داده‌ها، از جمله تجمیع آن‌ها از هر منبع(های) داده‌ای فقط برای استفاده قانونی کسب‌وکار است.
گزینه‌های مدیریت داده‌ها	*استخراج ارزش از داده‌ها:* – تجزیه و تحلیل کلان داده‌ها – داده‌های کسب‌وکار از حسگرها – یادگیری ماشینی و هوش مصنوعی (AI)		*ارائه صحت اطلاعات:* – مدیریت فراداده –اصالت‌سنجی داده		*مدیریت دیتاست‌ها:* – تجمیع داده‌ها – ترکیب دیتاست‌های داخلی و خارجی

[1] Data in context

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
	– هوش تجاری				
نظارت بر عملکرد و انطباق	*اطمینان از تجزیه و تحلیل داده‌ها به منظور حداکثر ارزش* – مدل تجزیه و تحلیل داده‌ها برای کسب‌وکار آماده و مناسب است		*حصول اطمینان از کاهش ریسک مرتبط با گزارش* – گزارش داده‌ها با هدف کسب و کار هماهنگ است		*حصول اطمینان از دانش کافی کارکنان برای گزارش‌دهی* – توانایی تهیه گزارش داده
استانداردهای مرتبط					*ISO/IEC 20889، در مورد تکنیک‌های عدم شناسایی داده‌ها برای افزایش حریم خصوصی

جدول ۵- تصمیم‌گیری (Decide)

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
V4	**بدنه حکمرانی باید اطمینان حاصل کند که فرهنگ داده سازمان با استراتژی داده‌های سازمان مانند شیوه‌های دسترسی به داده، تصمیم‌گیری مبتنی بر داده و یادگیری سازمانی (از فرآیند تصمیم‌گیری) هماهنگ است.**	**R4**	**داده‌ها و فرمت مناسب باید در یک گزارش برای تصمیم‌گیری خودکار یا انسانی ارائه شوند. در حالی که بدنه حکمرانی در قبال این تصمیمات پاسخگو است، باید مسئولیت‌های تصمیم‌گیری را برای سازمان و برای سطح قابل قبولی از ریسک داده‌ها تفویض کند**	**C4**	**خروجی فرآیند تصمیم‌گیری، به‌عنوان داده‌های جدید، ارزش، ریسک و محدودیت‌های خاص خود را خواهند داشت – و بدنه حکمرانی باید انتظارات فرآیند تصمیم‌گیری و مسئولیت‌های مرتبط را تعیین کند.**
تمرکز سیاست (خط‌مشی)	*V1 + فرهنگ داده برای سازمان.* به عنوان مثال: تصمیمات و داده‌های مرتبط با آنها باید برای بهبود چرخه یادگیری جمع‌آوری شوند.		*R1 + V1 + تفویض اختیار مناسب.* به عنوان مثال: تصمیمات، چه انسانی و چه خودکار، نمی‌توانند از اختیارات تخصیص داده شده به مسئولین تصمیمات فراتر رود.		*انتظارات از فرآیند تصمیم‌گیری* به عنوان مثال: برای اطمینان از تصمیمات خوب (و قابل دفاع)، این تصمیمات باید با استفاده از داده‌های معتبر گرفته شوند.
گزینه‌های مدیریت داده‌ها	*داده‌ها برای تصمیم‌گیری* – ارائه گزارش‌ها و فیدهای داده[1] به کاربران نهایی – دستیاران هوش مصنوعی		*تفسیر گزارش‌ها* – تعصبات و تبعیض – تصمیم‌گیری خودکار		*یادگیری سازمانی* – گزارش حلقه بسته[2] – سیستم‌های یادگیری
نظارت بر عملکرد و انطباق	*اطمینان از فرمول‌بندی فرهنگ داده برای تصمیمات مبتنی بر داده*		*حصول اطمینان از کاهش ریسک برای تصمیمات مبتنی بر داده*		*اطمینان از تصمیم‌گیری فرد مناسب (درست و مرتبط)*

[1] Data feeds
[2] Closed loop reporting

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
	- مکانیزم تصمیم‌گیری بر اساس فرهنگ داده		- فرآیند تصمیم‌گیری باید نظارت شود		- مسئولیت تصمیم‌گیری باید ثبت شود
استانداردهای مرتبط					

جدول ۶- توزیع / انتشار (Distribute)

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
V5	**بدنه حکمرانی باید سیاستی برای توزیع داده‌ها ایجاد کند که مطابق برنامه استراتژیک سازمان است.**	**R5**	**بدنه حکمرانی باید اطمینان حاصل کند که مدیران، کنترل‌های کافی را برای جلوگیری از توزیع نامناسب داده اعمال کرده‌اند.**	**C5**	**بدنه حکمرانی باید اطمینان حاصل کند که حقوق قانونی توزیع داده‌ها اجرا شده و توسط اشخاص ثالث رعایت می‌شوند.**
تمرکز سیاست (خط‌مشی)	*V1+ خط مشی توزیع داده.* به عنوان مثال: هنگامی که مشتریان محصول ما را می‌خرند، داده‌های مربوط به تحویل و استفاده از محصول را نیز دریافت می‌کنند.		*کنترل‌های کافی (مناسب).* به عنوان مثال: داده‌هایی که می‌توانند بدون هیچ هزینه‌ای به اشتراک گذاشته شوند، فقط از طریق پارتیشن شبکه « data sharing» در دسترس خواهند بود. اشتراک داده‌های پولی دارای ارزش و ریسک بالاتری هستند و فقط از طریق پارتیشن شبکه «data subscription» توزیع می‌شوند		*حقوق قانونی توزیع مناسب، شامل ورودی و خروجی.* به عنوان مثال: تنها زمانی می‌توان داده‌ها را با تامین‌کنندگان به اشتراک گذاشت که توافقنامه محرمانه وجود داشته باشد.
گزینه‌های مدیریت داده‌ها	*گزینه‌های توزیع داده‌ها* - فیدهای داده (RSS، oData، وب سایت ها، دانلودها) - هشدارهای ایمیل[1] برای مشتریان و تامین‌کنندگان		*ISMS* - ابزارهای هشداردهنده برای مدیریت		*مدیریت مسائل مربوط به حقوق داده‌ها* - حق چاپ، صدور مجوز - مدیریت دارایی نرم‌افزار
نظارت بر عملکرد و انطباق	*اطمینان از ارزشمند بودن داده‌های توزیع شده برای مشتریان* - توزیع بر اساس گزینه‌های (روش‌های) مناسب انجام می‌گیرد. - مخاطب به توزیع نیاز دارد.		*اطمینان از اینکه توزیع داده‌ها تحت کنترل است.* - گزارش‌های هشدار را به طور منظم نظارت و بررسی کنید		*حصول اطمینان از اینکه توزیع داده‌ها براساس قوانین انجام می‌گیرد.* - همه‌ی توزیع‌ها باید مطابق با سیاست حفظ حریم خصوصی انجام گیرد.

[1] Email alerts

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
استانداردهای مرتبط					*ISO/IEC 19770، در مورد مدیریت دارایی نرم‌افزار

جدول ۷- وارهایی (Dispose)

	ارزش (Value)		مخاطره (Risk)		محدودیت‌ها (Constraints)
V6	**بدنه حکمرانی باید سیاست‌هایی را برای وارهایی داده‌ها زمانی که دارای ارزش نیستند یا دیگر نمی‌توان آن‌ها را نگهداری کرد، تصویب کند.**	**R6**	**بدنه حکمرانی باید مدیران را به اجرای یک فرآیند وارهایی داده مناسب هدایت کند که شامل کنترل‌هایی مانند تخریب[1] امن و دائمی داده‌ها می‌شود.**	**C6**	**بدنه حکمرانی باید تعهدات نگهداری و وارهایی داده‌ها را نظارت کند و اطمینان حاصل کند که فرآیندهای کافی اجرا شده است.**
تمرکز سیاست (خط‌مشی)	*V1* به عنوان مثال: داده‌هایی که نادرست یا قدیمی هستند باید تصحیح یا حذف (وارها) شوند.		*R2 + فرآیند مناسب* به عنوان مثال: برای کاهش خطر افشا، اطلاعات شخصی مشتری باید ظرف ۱۸ ماه از زمانی که مشتری دیگر از خدمات ما استفاده نمی‌کند، از سیستم‌های ما حذف شوند.		*R2 + C5 + فرآیندهای کافی* به عنوان مثال: یک دپارتمان حقوقی، تغییرات در قوانین و مقررات حفظ داده‌ها را به مدیر عامل (CEO) اطلاع خواهد داد. چنین بررسی‌هایی باید در فواصل زمانی مشخص و کمتر از یک سال انجام گیرد.
گزینه‌های مدیریت داده‌ها	*ارزش وارهایی داده‌ها* - ابزارهای وارهایی داده‌ها را انتخاب کنید.		*مدیریت وارهایی داده‌ها* - افراد، فرآیندها، فناوری‌ها - اطمینان از وارهایی در فضای ابری		*مدیریت فرآیندهای نگهداری و وارهایی داده‌ها* - ردیابی فراداده‌ی داده‌های مورد نیاز برای نگهداری
نظارت بر عملکرد و انطباق	*اطمینان از اجرای یک روش تایید شده برای وارهایی داده‌ها* - بررسی (بازنگری) رویه (پروسیجر)		*حصول اطمینان از کنترل و همسویی فرآیند وارهایی با خط مشی ریسک سازمانی.* - بررسی(بازنگری) شواهد وارهایی داده‌ها		حصول اطمینان از اینکه وارهایی داده‌ها مطابق الزامات قانونی و مقرراتی انجام می‌گیرد. - بازنگری(بررسی) قوانین و مقررات مرتبط
استانداردهای مرتبط			*ISO/IEC 19086 در مورد SLA رایانش ابری *ISO/IEC 29100 در مورد چارچوب حریم خصوصی		

[1] Destruction

۴-۶- بکارگیری راهنماهای استاندارد ISO/IEC 38505-1 و ISO/IEC 38505-2 - مثال کافی‌شاپ

۴-۶-۱- کلیات

در این بخش در قالب یک مثال ساختگی سعی می‌شود چگونگی به کارگیری راهنماهای مطرح شده در استانداردها و در نتیجه توسعه نتایج استراتژیک تشریح شود.

۴-۶-۲- شرح مسئله

شرکت ECS با هدف ارائه خدمات خوب و محصولات با کیفیت به مشتریان در قالب ۵۰ کافی شاپ در سراسر کشور مشغول به فعالیت است. هیئت مدیره این شرکت از ۵ عضو تشکیل شده است که طی بازدید اخیر آن‌ها از فروشگاه، فرصت‌هایی برای توسعه کسب‌وکار شناسایی شده است. با بررسی‌های به عمل آمده مشخص شده که بسیاری از مشتریان ECS برای رسیدن به این کافی‌شاپ از کنار کافی‌شاپ‌های مشابه عبور می‌کنند. مشتریان در ECS می‌توانند قهوه مورد علاقه خود را خیلی سریع سرو کنند تا جایی که قهوه‌چی نام اکثر مشتریان و قهوه مورد علاقه آن‌ها را می‌شناسد. با وجود علاقه مشتریان به قهوه‌های این شرکت، اما سود شرکت پس از زمان پیک صبح‌گاهی کاهش می‌یابد. پس از بررسی‌های به عمل آمده مشخص می‌شود که عمده مشتریان کارمندانی هستند که در طول روز به جای بازگشت به ECS، از دستگاه‌های قهوه‌ساز در دفتر خود استفاده می‌کنند. پس از گفتگو با مشتریان معلوم شد مشکل زمان پیاده‌روی به ECS یا حتی زمان صرف قهوه مورد علاقه‌شان نیست بلکه آنها نمی‌توانند ریسک انتظار در صف طولانی سفارش را بپذیرند.

راه حل ساده یکی از مدیران این شرکت این است که تصاویر دوربین امنیتی که در فروشگاه موجود است از طریق اینترنت در اختیار مشتریان قرار داده شود تا از آن طریق مشتریان بتوانند طول صف را خودشان رصد کنند و در زمان مناسب به کافی‌شاپ رجوع کنند. به این ترتیب هم درآمد ECS افزایش می‌یابد و هم مشکل مشتریان حل می‌شود. آیا مشکل همچنان وجود دارد یا حل شد؟؟

اما در این راه حل، مسائل متعددی مطرح است. اولین موضوع امنیت و شاید حریم خصوصی باشد. کسب رضایت از تمام مشتریان برای تصویربرداری آنها به دلیل مسائل امنیتی و مهمتر از آن کسب رضایت برای قرار دادن تصاویر روی اینترنت عملا قابل قبول و امکان‌پذیر نیست. پس از بررسی جزئیات مشخص می‌شود مسئله آنها یک ابتکار کسب‌وکار استراتژیک مبتنی بر

داده است. به بیان دیگر، افزایش فروش پس از ساعات پیک صبحگاهی نیازمندان دادن اطلاعات بیشتر به مشتریان در مورد وضعیت کافی‌شاپ است.

به این ترتیب هیئت مدیره به بحث و تبادل نظر در خصوص احتمالات استراتژیک موجود می‌پردازند. در واقع طول صف در فروشگاه تنها یک داده‌ای بودکه ECS تمایل داشت به مشتریان خود به اشتراک بگذارد. اما ECS چه داده‌های دیگری را می‌تواند و در اختیار چه کسانی می‌تواند قرار دهد؟ آیا می‌توان به داده‌ها به عنوان عنصر اضافی برای پیشبرد کسب‌وکار نگاه کرد؟

از آن‌جایی که هیئت مدیره از ISO/IEC 38500 برای اطمینان از رفتارهای صحیح در مورد حکمرانی IT استفاده می‌کردند تصمیم می‌گیرند از ISO/IEC 38505-1 برای بررسی حکمرانی داده‌ها استفاده کند. در واقع هیئت مدیره با به‌کارگیری راهنماهای ISO/IEC 38505-1 درک کردند که چگونه می‌توانند اهداف سازمانی خود را از طریق یک استراتژی داده و چارچوب حکمرانی داده ارائه کنند (همانطور که در جدول ۸ نشان داده شده است)

جدول ۸- نمونه اهداف سازمانی

کافی شاپ نمونه جامعه شما، قهوه شما	**هدف سازمانی ECS** هدف ECS ایجاد محیطی دوستانه و شبیه خانه برای مشتریان است تا ضمن احساس راحتی، از غذا و نوشیدنی سالم استفاده کنند. آنها از خرید کالا در فروشگاه‌های ما احساس خوبی دارند زیرا می‌دانند که ما از ارزش‌های آنها در تجارت منصفانه، محصولات تازه و حمایت از جامعه و محیط زیست حمایت می‌کنیم. **استراتژی سازمانی ECS** استراتژی حول سه محور زیر می‌چرخد: - راحت باش (احساسی شبیه خانه) - خدمات شخصی - غذای سریعتر - تحویل غذا فراتر از محله (سفارش و تحویل برای مشتریان در فاصله ۲۰۰ متری) - جلساتی با منافع مشترک (استفاده از خریدها برای کلوب‌های اجتماعی) - اهداف سبک زندگی - بازی‌سازی سلامت (کالری، قند، اهداف سلامت، وعده‌های غذایی متعادل) - از خرید احساس خوبی داشته باشید - غذای من را به اشتراک بگذارید (یک ابتکار خیریه) - **استراتژی داده ECS** استراتژی داده ECS با اجرای این "۳ محور" و امکان ابتکارات آتی با ریسک کم برای مشتریان و تامین‌کنندگان، از هدف و استراتژی سازمانی پشتیبانی می‌کند. مزیت رقابتی ECS کسب رتبه اول بازار با یک سیستم مبتنی بر دانش و فرآیندهایی است که در آن، مشتریان برای دستیابی به اهداف سبک زندگی خود و حمایت از دیگران، مورد استقبال و پاداش قرار می‌گیرند.

۴-۶-۳- به کارگیری راهنماها

در جدول ۹ سوالاتی که هیئت مدیره براساس استانداردهای 38505-1 و 38505-2 به آنها پرداخته‌اند و اینکه چگونه این پرسش‌ها به سیاستی تبدیل می‌شود که از استراتژی جدید داده‌ی شرکت پشتیبانی می‌کند، آورده شده است.

در این مثال خطمشی مورد نیاز برای جمع‌آوری داده‌ها آورده شده است، که این فرآیند برای پنج حوزه‌ی دیگر در نقشه پاسخگویی داده‌ها می‌تواند تکرار شود.

جدول ۹- کاربرگ سیاست جمع‌آوری داده (مثال)

	ارزش(Value)	مخاطره(Risk)	محدودیت‌ها(Constraints)
جمع‌آوری (collect)	**بدنه حکمرانی باید تصمیم بگیرد که سازمان تا چه میزان از داده‌ها در راستای دستیابی به اهداف استراتژیک خود استفاده یا درآمدزایی کند.**	**بدنه حکمرانی باید مخاطرات مربوط به جمع‌آوری و استفاده از داده‌ها را بشناسد و با سطح قابل قبولی از ریسک داده‌ها مطابق چارچوب ریسک‌پذیری سازمان موافقت کند. این باید شامل بررسی مخاطرات ناشی از عدم جمع‌آوری و استفاده از داده‌ها نیز می‌شود.**	**بدنه حکمرانی باید سیاست‌های جمع‌آوری داده‌ها را با در نظر گرفتن محدودیت‌هایی مانند کیفیت، حریم خصوصی، الزامات رضایت و شفافیت استفاده تأیید کند.**
تمرکز سیاست (خطمشی)	*داده‌های مشتری یک منبع کلیدی هستند:* – داده ها باید دقیق باشند. – مشتری می تواند داده‌های مربوطه از جمله اولویت‌ها و اهداف و علایق سبک زندگی را ببینند و به روز کند. *داده‌های محصول و زنجیره تامین اجزای اصلی هستند.* *داده‌های اضافی (مانند آب‌وهوا، ترافیک، امور خیریه) را می‌توان به طور مناسبی انتخاب و گردآوری کرد.*	*کیفیت و دقت داده‌ها باید در بین مجموعه داده ها همسو و سازگار[1] باشند.* *داده های مشتری یک دارایی کلیدی است و باید به طور ایمن جمع آوری شود*	*قبل از جمع آوری باید از مشتریان رضایت گرفته شود.* *PII مشتری فروخته نخواهد شد.* *ما از داده‌های خود برای شراکت با سازمان های خیریه تایید شده استفاده می‌کنیم، اما از آنها سود نمی بریم*

[1] Consistent

گزینه‌های (آپشن) مدیریت داده‌ها	*گزینه‌های جمع‌آوری داده‌ها:* – دستگاه هوشمند – به روزرسانی‌های برنامه – مجموعه سنسورها *گزینه‌های شناسایی مشتری* *گزینه های تجمیع و تقویت (افزایش):* – آیا می‌توان داده‌ها را جمع‌آوری کرد؟ – آیا می‌توانیم (و می‌خواهیم) مشتریان خود را شناسایی کنیم؟ – به چه نوع داده‌هایی نیاز داریم؟ – چگونه می‌توانیم داده‌ها را به طور موثر جمع‌آوری کنیم؟	– چه فرآیندها و کنترل‌هایی برای محافظت از داده‌ها وجود دارد؟ – چه کسی مسئول داده‌های مشتری است؟ – چه تعاریفی باید ارائه شود؟ – چه نوع مسئولیت‌هایی باید تایید شوند؟ – چگونه می‌توانیم از صحت داده‌ها اطمینان حاصل کنیم؟	– آیا می‌توانیم به درستی تشخیص دهیم PII چیست؟ – اگر PII را جمع‌آوری کنیم، برای هر بازاری که در آن فعالیت می‌کنیم باید از چه قوانینی پیروی کنیم؟ – چه نوع فناوری برای جمع‌آوری داده‌ها باید پذیرفته شود؟ – برای اطمینان از اینکه به عنوان یک متصدی اطلاعات خوب عمل می‌کنیم، به چه سیاست‌های دیگری نیاز داریم؟
مثال کافی‌شاپ بیانیه‌های سیاست	**ساختار سازمانی** *هیئت مدیره باید از ایجاد ساختار سازمانی مورد نیاز برای جمع‌آوری کارآمد داده‌ها، ازجمله مسئولیت‌های دپارتمان، پست‌ها و مسئولیت‌های فردی اطمینان حاصل کند.* به عنوان مثال: – شناسایی بخش‌هایی که در جمع‌آوری داده‌ها نقش دارند. – شناسایی سمت‌ها و مسئولیت‌های مرتبطی که باید در بخش‌های مرتبط با جمع‌آوری داده‌ها ایجاد شوند. – لازم به ذکر است مسئول حفظ حریم خصوصی مسئولیت اطمینان از کسب رضایت مشتریان قبل از جمع‌آوری داده‌های آن‌ها را دارد. **ارزش** *هیئت مدیره باید تصمیم بگیرد که سازمان تا چه میزان از داده‌ها برای دستیابی به اهداف استراتژیک خود استفاده یا درآمدزایی کند.* **ریسک** هیئت مدیره باید ریسک‌های مرتبط با جمع‌آوری داده‌ها را بشناسد و با سطح قابل قبولی از ریسک داده‌ها در چارچوب ریسک‌پذیری سازمان موافقت کند. این باید شامل بررسی مخاطرات ناشی از عدم جمع‌آوری و استفاده از داده‌ها نیز می‌شود. به عنوان مثال: – هیئت مدیره در مورد سطح ریسکی که سازمان برای دستیابی به اهداف استراتژیک خود آماده انجام آن است، تصمیم می‌گیرد. – داده‌های دقیق، مانند داده‌های مکانی یا آدرس، فقط از مشتریان پرداخت‌کننده جمع‌آوری می‌شوند.		

	– روش مناسب برای اثبات صحت داده‌ها استفاده خواهد شد. – ممیزی جمع‌آوری داده‌ها هر نیم سال یکبار انجام خواهد شد. **محدودیت‌ها** هیئت مدیره باید سیاست‌های جمع‌آوری داده‌ها را با در نظر گرفتن محدودیت‌هایی مانند کیفیت، حفظ حریم خصوصی، الزامات رضایت و شفافیت کاربرد تأیید کند. به عنوان مثال: – مقررات و قوانین مربوط به جمع‌آوری داده‌ها که باید توسط سازمان رعایت شوند، شناسایی خواهند شد. به عنوان مثال، برای جمع‌آوری PII، قوانین خاصی باید برای جمع‌آوری داده‌ها وجود داشته باشد تا از انطباق با قوانین حفظ حریم خصوصی اطمینان حاصل شود. – این سیاست باید شامل مقررات بازار منطقه‌ای باشد و اطمینان حاصل شود که سختگیرانه‌ترین الزامات در هر منطقه اتخاذ می‌شود (مثلاً در اروپای غربی، سازمان از قوانین آلمان تبعیت می‌کند مگر اینکه خلاف آن ذکر شده باشد). – PII نباید از افراد زیر ۱۵ سال جمع‌آوری شود. – تمام داده‌های جمع‌آوری شده برای انتقال رمزگذاری می‌شوند
نظارت بر عملکرد و انطباق	هیئت مدیره باید انطباق مربوط به جمع‌آوری داده‌ها، از جمله آماده‌سازی، پیاده‌سازی و تکمیل جمع‌آوری داده‌ها را نظارت کند. به عنوان مثال: — در مرحله آماده‌سازی، محدوده، شیء (آبجکت)، روش و سایر وظایف جمع‌آوری داده‌ها مشخص خواهند شد. – فرآیندهای جمع‌آوری ایجاد و تصویب خواهند شد. – رویه‌های جمع‌آوری و مسئولیت‌های مرتبط برای اهداف ممیزی IT ردیابی می‌شوند. – رویه‌های جمع‌آوری هر نیم سال بازنگری خواهند شد

۵- نقشه‌راه استانداردسازی حکمرانی داده کانادا

۵-۱- چکیده اجرایی

در نوامبر ۲۰۲۰، دولت کانادا اساسنامه (منشور) اجرایی دیجیتال را با هدف ایجاد استراتژی داده‌ی ملی برای بهره‌گیری از مزایای اقتصادی نشأت گرفته از داده پیشنهاد کرد. در این راستا، ائتلاف تدوین استاندارد حکمرانی داده کانادا (DGSC) به منظور ایجاد هماهنگی بین برنامه‌های توسعه و سازگاری استانداردهای حکمرانی داده و برنامه‌های ارزیابی انطباق تکمیلی[1]

[1] Complementary conformity assessment

در کانادا راه‌اندازی شد. این سند (نقشه‌راه) اولین خروجی این ائتلاف است که بر روی زنجیره ارزش حکمرانی داده به منظور توصیف چشم‌انداز حال و مطلوب استانداردسازی کانادا متمرکز شده است و شامل توصیه‌هایی برای برطرف کردن شکاف‌ها و شناسایی حوزه‌های جدید برای دولت کانادا می‌شود.

۵-۲- شناسایی موضوعات کلیدی

در ژانویه ۲۰۲۰، حوزه‌های اولویت‌دار برای نقشه‌راه به ۳۵ موضوع اختصاص داده شد (با ذکر این نکته که این نقشه‌راه قادر به رسیدگی به تمام مسائل مربوط به پیچیدگی‌های حکمرانی داده نخواهد بود). لازم به ذکر است حکمرانی داده می‌تواند از طریق مدل‌ها و جنبه‌های متفاوتی بررسی شود.

در این سند، فعالیت‌های حکمرانی داده در چهار حوزه گسترده و متعاقباً به چهار گروه کاری تقسیم شده است:

۱) مبانی حکمرانی داده

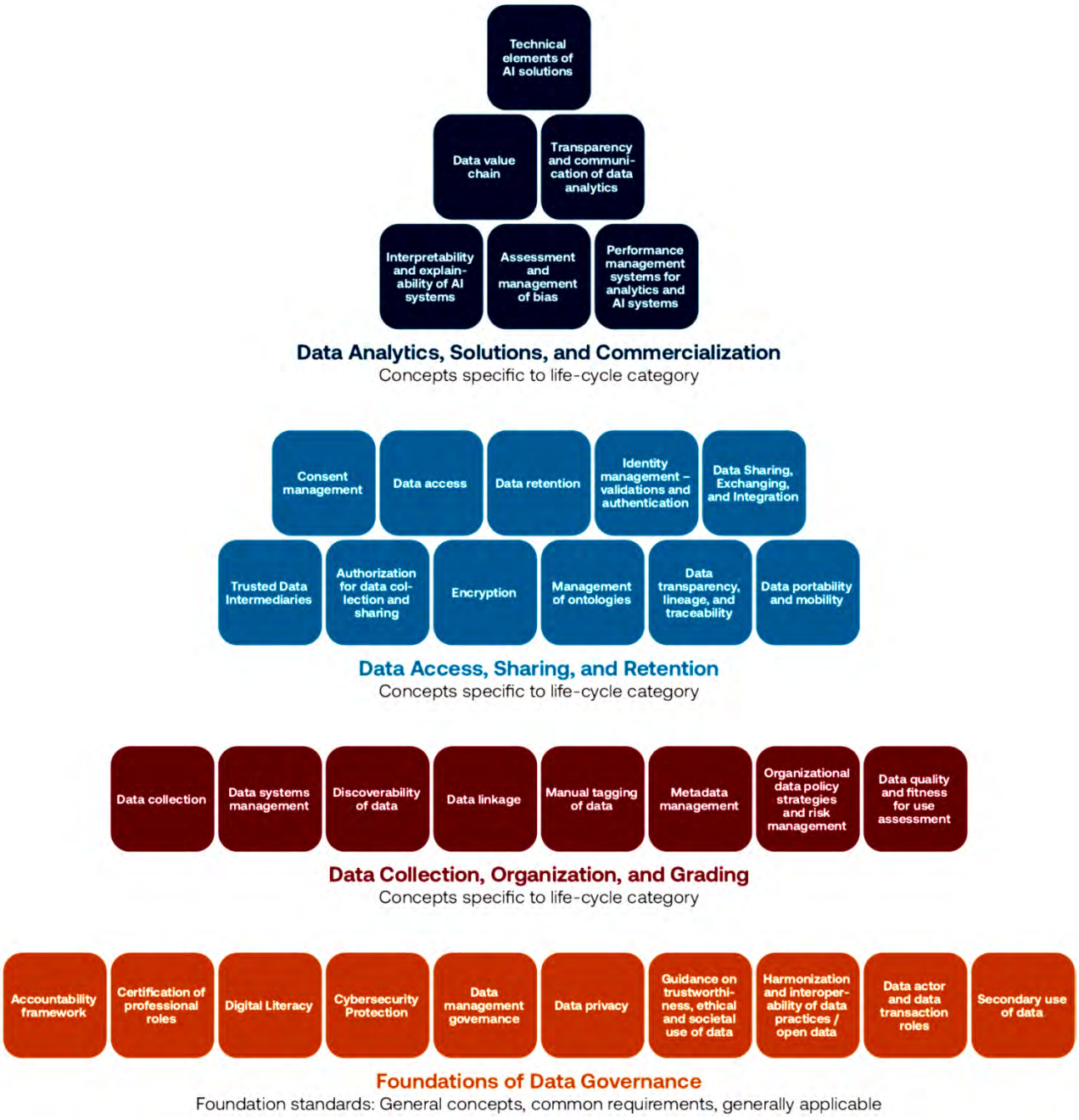
۲) جمع‌آوری، سازماندهی و درجه‌بندی[1] داده‌ها

۳) دسترسی به داده‌ها، به اشتراک‌گذاری و نگهداری آن‌ها

۴) تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها.

در هریک از این حوزه‌ها، موضوعات گسترده‌ای مرتبط با استانداردها و برنامه‌های ارزیابی انطباق برای حکمرانی داده شناسایی شده‌اند که در شکل زیر نشان داده شده‌اند.

[1] Grading



شکل ۱۴- حوزه‌ها و موضوعات کلیدی حکمرانی داده

در جدول زیر معادل‌های فارسی هر یک موضوعات به تفکیک کارگروه‌ها به منظور خوانایی بیشتر قرار داده شده است.

جدول ۱۰- حوزه‌ها و موضوعات کلیدی حکمرانی داده

کارگروه ۱: مبانی حکمرانی داده‌ها	تعهدپذیری (پاسخگویی)
	گواهی برای نقش‌های تخصصی
	سواد (دانش) دیجیتال
	حفاظت از امنیت سایبری
	حکمرانی مدیریت داده
	حریم خصوصی (تلقیق شده با موضوع حقوق داده‌ها)
	راهنمایی بر استفاده قابل اعتماد، اخلاقی و اجتماعی از داده‌ها
	هماهنگی و قابلیت همکاری اقدامات داده/ داده باز
	بازیگران داده و نقش‌های تراکنش‌های داده
	کاربردهای (ثانوی از) داده‌ها
کارگروه ۲: جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها	جمع‌آوری (گردآوری) داده‌ها
	مدیریت سیستم‌های داده
	قابلیت کشف داده‌ها
	پیوند(لینک کردن) داده‌ها
	برچسب‌گذاری دستی داده‌ها
	مدیریت متادیتا
	استراتژی‌های خط‌مشی داده‌های سازمانی و مدیریت مخاطره (ریسک)
	ارزیابی کیفیت و تناسب داده‌ها برای استفاده (کاربرد)
کارگروه ۳: دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها	مدیریت رضایت (رضایت، دسترسی و برداشت از داده‌ها)
	دسترسی به داده‌ها
	نگهداری داده‌ها
	مدیریت هویت–اعتبارسنجی و احراز هویت (افراد، نهادها و دستگاه‌ها)
	به اشتراک‌گذاری، تبادل و یکپارچه‌سازی داده‌ها

	واسطه‌های قابل اعتماد داده‌ها
	مجوز به اشتراک‌گذاری و جمع‌آوری (گردآوری) داده‌ها
	رمزنگاری
	مدیریت هستی‌شناسی (فهرستی از مفاهیم و دسته‌بندی‌های داده و ارتباط بین آن‌ها)
	قابلیت ردیابی، اصل و ریشه (وابستگی به داده‌های گذشته) و شفافیت داده‌ها
	قابلیت جابه‌جایی و حمل داده‌ها
کارگروه ۴: تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها	مؤلفه‌های فنی راه حل‌های هوش مصنوعی
	زنجیره ارزش داده‌ها
	شفافیت و ارتباط تجزیه‌وتحلیل داده‌ها
	تفسیرپذیری و توضیح‌پذیری سیستم‌های هوش مصنوعی (تفسیرپذیری الگوریتم‌ها)
	ارزیابی و مدیریت سوگیری (غرض‌ورزی)
	سیستم‌های مدیریت کارایی برای سیستم‌های هوش مصنوعی و تجزیه‌وتحلیل

در ادامه این سند برای موضوعات مطرح شده در هریک از چهار کارگروه معرفی شده توضیح مختصری از محدوده (گستره)[1] موضوع، وضعیت (داستان) کاربر[2]، و توصیه[3] (راه حل‌های استانداردسازی برای کانادا) ارائه شده است. برای مثال در کارگروه ۱: مبانی حکمرانی داده؛ موضوع ۱: چارچوب پاسخگویی (Accountability Framework) توضیحات زیر آورده شده است:

– محدوده (دامنه) موضوع: ساختار کنترل و مسئولیت برای تمام داده‌های جمع‌آوری شده و ایجاد شده شامل نقش‌ها، مسئولیت‌ها و پاسخ‌دهی به تراکنش‌های داده (از جمله مسئولیت دارندگان یا صاحبان امتیاز حقوق داده، پیامدهای انتقال مالکیت، مفهوم رضایت، انطباق و پاسخگویی از طریق مقررات.)

– داستان کاربر: به عنوان یکی از والدین کانادایی که فرزندان آن‌ها از محیط‌های آموزش الکترونیکی استفاده می‌کند، لازم است شفافیت در مورد نحوه موافقت والدین از پلتفرم‌های یادگیری آنلاینی که فرزندانشان از آن‌ها استفاده می‌کنند و همچنین نحوه جمع‌آوری و استفاده از داده‌های آن‌ها برای مقاصد دیگر وجود داشته باشد. چگونه والدین می‌توانند اطمینان حاصل کنند که این پلتفرم‌ها منطبق با مقررات حریم خصوصی است؟

[1] Scope
[2] User story
[3] Recommendation

– توصیه: توسعه بهترین اقدامات ملی و/ یا راه‌حل‌های استانداردسازی برای چارچوب‌های پاسخگویی (مسئولیت‌پذیری) مرتبط با حریم خصوص و امنیت اطلاعات شخصی

زمان‌بندی پیاده‌سازی این نقشه‌راه (ترتیب اجرایی) به صورت حدودی شامل پیاده‌سازی توصیه‌های ارائه شده برای هریک ازموضوعات کلیدی در جدول ۱۱ نشان داده شده است.

در بخش دیگری از این سند (نقشه‌راه) شرحی از مسائل کلیدی، استانداردها و مشخصه‌های منتشر شده و یا در حال توسعه مرتبط ارائه شده است. همچنین توصیه‌هایی در مورد نیاز به تحقیق و توسعه و/ یا استانداردها و مشخصه‌های بیشتر و اولویت‌بندی توسعه آن‌ها و سازمان‌هایی که به طور بالقوه مسئول انجام وظایف هستند، آورده شده است. به عنوان نمونه‌ای از این سند، توضیحات مرتبط با کارگروه ۱: مبانی حکمرانی داده، موضع ۱: چارچوب پاسخگویی در ادامه آورده شده است.

شکاف چارچوب پاسخگویی: استانداردهای زیادی مرتبط با این موضوع وجود دارند با این وجود تعداد کمی از این استانداردها به عنوان مرتبط طبقه‌بندی شده‌اند. اکثر استانداردهای مرتبط با این موضوع مختص یک بخش خاص (عمدتاً بهداشت و حمل و نقل) هستند. نکته جالب توجه این است که بیش از نیمی از استانداردهای مرتبط در سال ۲۰۱۷ و بعد از آن منتشر شده‌اند که نشان‌دهنده تلاش فراوان برای ارائه ابزارهای استانداردسازی مناسب برای پاسخگویی بهتر در حکمرانی داده است. برای این موضوع شکاف مشخصی در بین استانداردها شناسایی نشد. چالش اصلی برای سازمان‌ها این است که قوانین مختلف حریم خصوصی داده‌ها که در حوزه‌های قضایی مختلف ظهور می‌کنند را رهیابی (هدایت) کنند و استانداردها را با این مقررات هماهنگ نمایند.

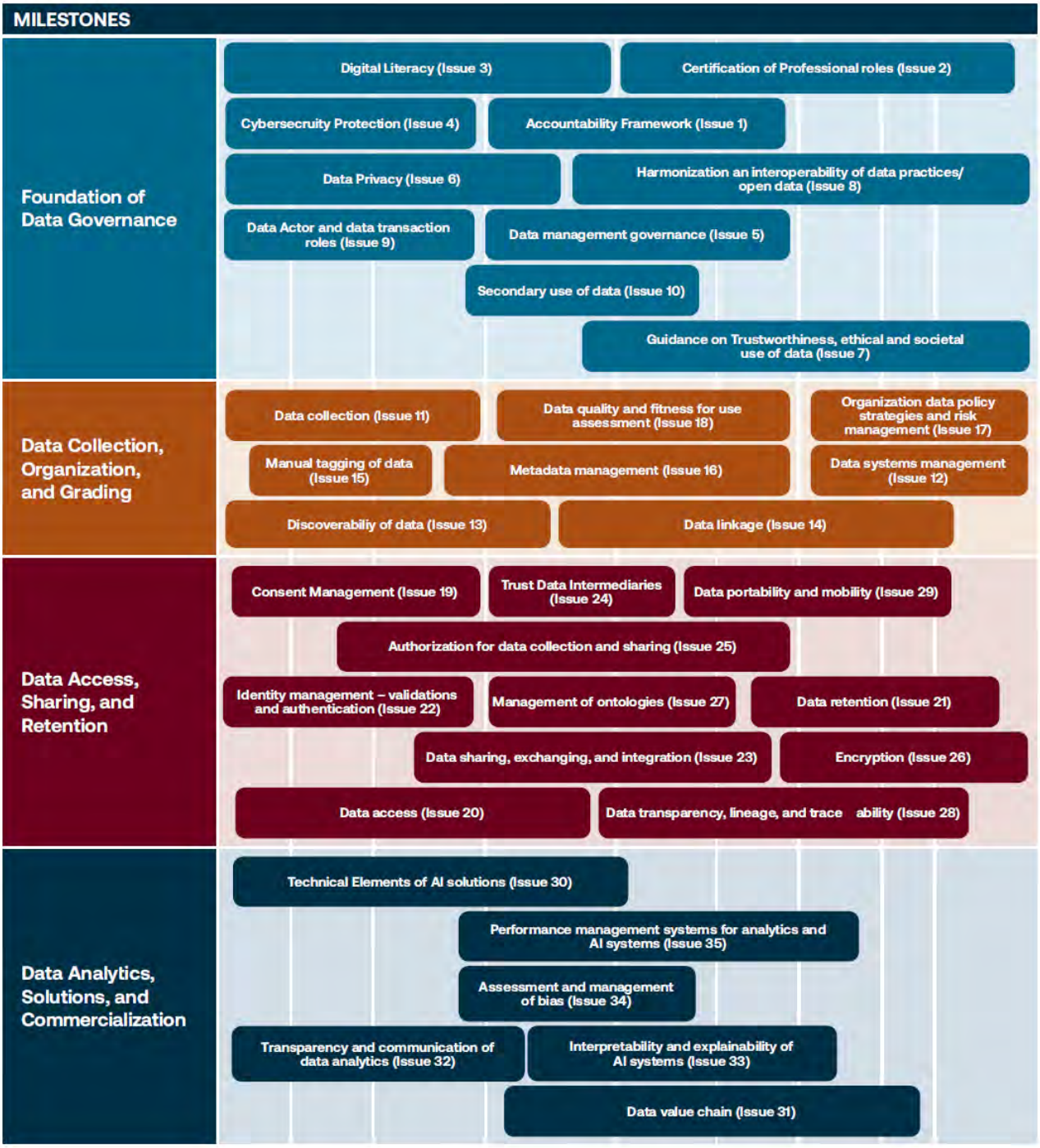
آیا نیاز به تحقیق و توسعه است؟ بله

توصیه: توسعه بهترین اقدامات ملی برای چارچوب‌های پاسخگویی مرتبط با حریم خصوصی و امنیت اطلاعات شخصی

اولویت: متوسط

سازمان(ها): دفتر رئیس کمیسیون اطلاعات و حریم خصوصی در حوزه‌های قضایی و در سطح فدرال

جدول ۱۱- زمان‌بندی پیشنهادی برای پیاده‌سازی نقشه‌راه



۵-۳- فهرست استانداردهای منتشر شده برای موضوعات کلیدی نقشه‌راه حکمرانی داده کانادا

در ادامه فهرست استانداردهای منتشر شده مرتبط با هر موضوع کلیدی به تفکیک قرار داده شده است.

همچنین خاطر نشان می‌گردد در سند نقشه‌راه استانداردسازی حکمرانی داده کانادا موضوعات دیگری از جمله نحوه نظرسنجی (بومی کانادا) در خصوص وضعیت موضوعات مطرح شده در کانادا توضیحاتی ارائه می‌شود و روش‌های استفاده شده برای مشارکت فعالیت‌ها شامل انتخاب ذی‌نفعان (مشارکت‌کنندگان)، تعداد مشارکت‌کنندگان از روش‌های مختلف و مهمترین کامنت‌های آن‌ها، موضوعات کلیدی در مصاحبات، توصیه‌ها، اسناد رضایت‌نامه آگاهانه (فرم رضایت‌نامه)، نظرسنجی (پرسشنامه)، راهنمای پرسشنامه، توصیف روش‌های مختلف مشارکت و روش‌های تحلیل معرفی می‌شوند. در بخش بعدی این نقشه‌راه به عنوان یک نمونه کاربردی، داده‌های بهداشت (سلامت) جامعه و استانداردسازی آن‌ها مورد بحث قرار میگیرد. چالش‌ها و وضعیت داده‌ها در هر یک از موضوعات مطرح در این نقشه‌راه مورد تحلیل قرار می‌گیرد و گزارشات کارگروه مربوطه ارائه می‌شود. همین روند برای نمونه‌های کاربردی دیگر شامل شناسایی دیجیتال و بانکداری باز، ایمنی و توانمندسازی مصرف‌کننده: زنجیره‌های تأمین مواد غذایی دیجیتال، سیستم‌های نظارت و آموزشی الکترونیکی کودکان بیان شده است. در انتها متدولوژی توسعه نقشه‌راه استانداردها و کارگروه‌های مربوطه معرفی می‌شوند.

دسته‌بندی استانداردهای موجود مطابق چارچوب استانداردسازی حکمرانی داده کانادا به تفکیک در چهار کارگروه (۱) مبانی حکمرانی داده؛ (۲) جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها؛ (۳) دسترسی به داده‌ها، به اشتراک‌گذاری و نگهدرای آن‌ها؛ (۴) تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها در ادامه آورده شده است.

۵-۳-۱- استانداردهای مرتبط با کارگروه ۱: مبانی حکمرانی داده

۵-۳-۱-۱- استانداردهای مبانی حکمرانی داده _ موضوع ۱: چارچوب تعهدپذیری (پاسخگویی)

Issue 1— Accountability Framework	
IEEE STDVA24228	Big Data Governance and Metadata Management: Standards Roadmap
ISO/TR 24514	Activities relating to drinking water and wastewater services – Examples of the use of performance indicators using ISO 24510, ISO 24511 and ISO 24512 and related methodologies
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
SAE GEIA-HB-859	Implementation Guide for Data Management – Formerly TechAmerica GEIA-HB-859

ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ITU-T H.860	Multimedia e-health data exchange services: Data schema and supporting services – Study Group 16
ITU-T Y.3514	Cloud computing – Trusted inter-cloud computing framework and requirements – Study Group 13
CEN/TR 17370	Public transport – Operating raw data andstatistics exchange
ISO 11240	Health informatics – Identification of medicinal products – Data elements and structures for the unique identification and exchange of units of measurement
ISO 15394	Packaging – Bar code and two-dimensional symbols for shipping, transport and receiving labels
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and dataprotection policies
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiable information protection
ISO/IEC 29187-1	Information technology – Identification of privacy protection requirements pertaining to learning, education and training (LET) – Part 1: Framework and reference model
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and dataprotection policies
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/IEC 29184:2020	Information technology – Online privacy notices and consent
ISO/IEC WD TS 27560	Privacy technologies – Consent record information structure
n/a	A Guide for Ethical Data Science
CAN/CIOSC 100-n	Series of standards for datagovernance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
IEEE P7002	Data Privacy Process

IEEE P7004	Standard for Child and Student Data Governance
IEEE P7005	IEEE Draft Standard for Transparent Employer Data Governance
IEEE P2089	Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children
IEEE P3800	Standard for adata-trading system: overview, terminology and reference model
IEEE P2895	Standard Taxonomy for Responsible Trading of Human-Generated Data
IC16-002	The Global Initiative on Ethics ofAutonomous and Inteligent Systems
IC19-004	Technology and Data Harmonization for Enabling Clinical Decentralized Clinical Trials
IC18-004	Ethics Certification Program for Autonomous and Inteligent Systems (ECPAIS)

۵-۳-۱-۲- استانداردهای مبانی حکمرانی داده _ موضوع ۲: گواهی برای نقش‌های تخصصی

Issue 2 — Certification for Professional Roles	
ETSI TR 103 370	Practical introductory guide toTechnical Standards for Privacy – V1.1.1

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
COBIT 2019	Effective IT Governance at Your Fingertips – Build your expertise in the globally accepted framework foroptimizing enterprise IT governance.
n/a	ISACA CREDENTIALS
CAN/CIOSC 100-n	Series of standards for datagovernance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CIOSC 102	Qualification and certification of bigdata and machine learning personnel
CAN/CIOSC 109-1	Qualification and proficiency of privacy and access control professionals
ISO/IEC/IEEE 24765:2017	International Standard – Systems and software engineering – Vocabulary

۵-۳-۱-۳- استانداردهای مبانی حکمرانی داده _ موضوع ۳: سواد (دانش) دیجیتال

Issue 3 — Digital Literacy	
ITU-T L.1505	Information and communication technology and adaptation of the fisheries sector to the effects of climate change– Study Group 5
ISO 21248	Information anddocumentation – Quality assessment for national libraries – First edition
ISO/IEC TR 18120	Information technology – Learning, education, and training – Requirements for e-textbooks in education – First Edition
ISO/IEC 18120	Information technology – Learning, education, and training – Requirements for e-textbooks in education
ISO/IEC 19788-5	Information technology – Learning, education and training – Metadata for learning resources Part 5: Educational elements
ISO/IEC TR 18120	Information technology – Learning, education, and training – Requirements for e-textbooks in education
BSI PAS 1040	Digital readiness – Adopting digital technologies inmanufacturing – Guide
BSI PAS 1296	Online age checking – Provision anduse ofonline age check services – Code of practice
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap Part 2: Architectural components and maturity model
DS DS/CWA 16213	End User e-Skills Framework Requirements
DS DS/CWA 16266	Curriculum for training ICT Professionals in Universal Design

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
n/a	Levelling Up: The Quest forDigital Literacy
n/a	Improving Canada's Digital Advantage: Building the Digital Talent Pool and Skills for Tomorrow
n/a	TELUS Wise
n/a	What is digital literacy?
n/a	Digital Literacy Framework Yukon Education
n/a	Elements of AI free online course
n/a	Certified Ethical Emerging Technologies
CAN/CIOSC 100-n	Series of standards for datagovernance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
IEEE 3527.1-2020	IEEE Approved Draft Standard for Digital Intelligence (DQ) – Framework for Digital Literacy, Skills and Rediness
IEEE P2089	Standard for AgeAppropriate Digital Services Framework – Based on the 5Rights Principles forChildren
IEEE P7011	Standard for the Process ofIdentifying andRating the Trustworthiness of News Sources

۵-۳-۱-۴- استانداردهای مبانی حکمرانی داده _ موضوع ۴: حفاظت از امنیت سایبری

Issue 4 — Cybersecurity Protection	
ISO/IEC 29100	Information technology – Security techniques – Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)
ISO/IEC TR 27103	Information technology – Security techniques – Cybersecurity and ISO and IEC Standards
CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
CENELEC EN 50584	Information technology – CENELEC/ETSI Glossary of terms and definitions for broadband deployment including sustainability aspects
CENELEC EN 50173-1	Information technology – Generic cabling systems Part 1:General requirements
CENELEC EN 50173-2	Information technology – Generic cabling systems – Part 2: Office spaces
CENELEC EN 50173-5	Information technology – Generic cabling systems Part 5:Data centre spaces
ISO/IEC 8348	Information technology – Open Systems Interconnection – Network service definition
ISO/IEC 17788	Information technology – Cloud computing – Overview andvocabulary
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ITU-T Y.3500	Information technology – Cloud computing – Overview andvocabulary – Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ISO/IEC 15504.5	Information technology – Process assessment Part 5: An exemplar software life cycle process assessment model
ISO/IEC 15504-5	Information technology – Process assessment Part 5: An exemplar software life cycle process assessment model
ISO/IEC 18028.2	Information technologySecurity techniquesIT network security Part 2: Network security architecture – ISO/IEC 18028-2:2006
ISO/IEC 19770-8	Information technology – IT asset management Part 8:Guidelines for mapping of industry practices to/ from the SO/IEC 19770 family of standards
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
ISO/IEC 27034-5	Information technology – Security techniques – Application security Part 5: Protocols and application security controls data structure
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29115	Information technology – Security techniques – Entity authentication assurance framework

ISO/IEC 29190	Information technology – Security techniques – Privacy capability assessment model
ISO/IEC 30100-2	Information technology – Home network resource management – Part 2: Architecture
ISO/IEC 30105-2	Information technology – IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes Part 2 Process assessment model (PAM)
ISO/IEC 38500	Information technology – Governance of IT for the organization
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to thegovernance of data
ISO/IEC 38506	Information technology – Governance of IT – Application of ISO/IEC 38500 to the governance of IT enabled investments
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 fordata management
ISO/IEC TS 27034-5-1	Information technology – Application security Part 5-1: Protocols and application security controls data structure, XML schemas
SNZ AS/NZS 15271	Guide for AS/NZS ISO/IEC 12207 (Information Technology) – Software Life Cycle Processes)
CEN EN 16571	Information technology – RFID privacy impact assessment process
ISO/IEC/IEEE 42030	Software, systems and enterprise – Architecture evaluation framework
CENELEC EN 50667	Information technology – Automated infrastructure management (AIM) systems – Requirements, data exchange and applications
ISO/IEC 18028-5	Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual privatenetworks
ISO/IEC 18043	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems
ISO/IEC 20243-2	Information technology – Open Trusted Technology ProviderTM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products Part 2: Assessment procedures for the O-TTPS and ISO/ IEC 20243-1:2018
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation of virtualized servers
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management –
ISO/IEC 27034-1	Information technology – Security techniques – Application security Part1: Overview and concepts – CORR: February28, 2014
ISO/IEC 27034-2	Information technology – Security techniques – Application security Part 2: Organization normative framework
ISO/IEC 27034-3	Information technology – Application security Part 3: Application security management process
ISO/IEC 27039	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS) – CORR: June 30,2018
ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment – CORR: April 30, 2020

ISO/IEC TR 13335-5	Information Technology – Guidelines for the Management of IT Security – Part 5: Management Guidance on Network Security (TECHNICAL REPORT)
ISO/IEC TR 14516	Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services (Technical Report)
ISO/IEC TR 15443-1	Information technology – Security techniques – Framework for IT security assurance – Part 1: Overview and Framework (Technical Report)
ISO/IEC TR 15443-2	Information technology – Security techniques – Security assurance framework – Part 2: Analysis (Technical Report)
ISO/IEC TR 15443-3	Information technology – Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods
ISO/IEC TR 19791	Information technology – Security techniques – Security assessment of operational systems (Technical Report)
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 29156	Information technology – Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
ISO/IEC TR 29181-5	Information technology – Future Network – Problem statement and requirements Part 5: Security
ITU-T STIT	Security inTelecommunications and Information Technology – Study Group 17
ITU-T X.842	Information technology – Security techniques – Guidelines for the use and management of trusted third party services – Study Group 7
ISO/IEC 27006	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
DIN SPEC 91367	Urban mobility data collection forreal-time applications; Text in English
ISO 14641	Electronic document management – Design and operation of an information system for the preservation of electronic documents – Specifications
ISO 29134	Information technology – Security techniques – Guidelines for privacy impact assessment (ISO/IEC 29134:2017)
ISO/IEC 10021-8	Information technology – Message Handling Systems (MHS) – Part 8: Electronic Data Interchange Messaging Service
ISO/IEC 18045	Information technology – Security techniques – Methodology for IT security evaluation
ISO/IEC 20944-1	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) Part 1: Framework, common vocabulary, and common provisions for conformance
ISO/IEC 23736-3	Information technology – Digital publishing – EPUB 3.0.1 Part 3: Content documents
ISO/IEC 27034-6	Information technology – Security techniques – Application security – Part 6: Case studies
ISO/IEC 27034-7	Information technology – Application security Part 7:Assurance prediction framework
ISO/IEC 29147	Information technology – Security techniques – Vulnerability disclosure
ISO/IEC 30111	Information technology – Security techniques – Vulnerability handling processes

ISO/IEC TS 19249	Information technology – Security techniques – Catalogue of architectural and design principles for secure products, systems and applications
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operational environment
ISO/IEC TS 22237-6	Information technology – Data centre facilities and infrastructures Part 6: Security systems
ISO/IEC 27033-5	Information technology – Security techniques – Network security Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
n/a	National Cyber Security Strategy
ISO 20252:2019	Market, opinion and social research, including insights and data analytics – Vocabulary and service requirements
ISO 19092:2008	Financial services – Biometrics – Security framework
ISO/TR 22100-4:2018	Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data deidentification framework
CIOSC/PAS 100-4:2020	Data governance – Part 4: Specification for Scalable Remote Access Infrastructure
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
CAN/CIOSC 103-3	Digital trust and identity – Part 3: Digital credentials
CAN/CIOSC 103-4	Digital trust and identity – Part 4: Digital wallets
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
CAN/CIOSC 105	Cybersecurity of Industrial Internet of Things (IIoT) devices and systems
IEEE P2658	Guide for Cybersecurity Testing in Electric Power Systems
IEEE P1547.3	Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
IEEE P2808	Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
IEEE P9274.4.2	Recommended Practice for Cybersecurity in the Implementation of the Experience Application Programming Interface (xAPI)
IEEE P2418.9	Standard for Cryptocurrency Based Security Tokens

IEEE P2933	Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security
IEEE P1609.2	Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages
IEEE P802.15.4y	IEEE Draft Standard for Low-Rate Wireless Networks Amendment Defining Support for Advanced Encryption Standard (AES)-256 Encryption and Security Extensions
IEEE P802.1AEdk	Standard for Local and metropolitan area networks-Media Access Control (MAC) Security Amendment 4: MAC Privacy protection
IEEE P1912	Standard for Privacy and Security Framework for Consumer Wireless Devices
IEEE P2621 series	Wireless Diabetes Device Security Assurance (3 projects under development)
IEEE P1711.1	Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links: Substation Serial Protection Protocol
IEEE P1686	Standard for Intelligent Electronic Devices Cyber Security Capabilities
IEEE 2030.102.1-2020	IEEE Approved Draft Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems
ISO/IEC 27400	Cybersecurity – IoT security and privacy – Guidelines
ISO/IEC 27402	Cybersecurity – IoT security and privacy – Device baseline requirements
ISO/IEC 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
CSA T100**	ICT Code for Buildings
CSA T200**	Evaluation of software development and cybersecurity programs (update to CSA EXP 200)
CSA EXP 200	Evaluation of software development and cybersecurity programs
CSA T2000-1**	Intelligent Building System Objective Code
CSA T2000-2**	Intelligent Building System Safety Management System Code
CSA Z246.1	Security management for petroleum and natural gas industry systems
CSA N290.7	Cyber security for nuclear power plants andsmall reactor facilities
CSA T150**	Connected and automated vehicle code
CSA T710**	Smart manufacturing readiness assessment methodology and requirements
CAN/CSA-ISO 14971	Medical Devices – Application of Risk Management to MedicalDevices
CAN/CSA-CEI/IEC 62304	Medical device software – Software life cycle processes

۵-۳-۱-۵- استانداردهای مبانی حکمرانی داده _ موضوع ۵: حکمرانی مدیریت داده

Issue 5 — Data Management Governance	
ISO/IEC TR 38505-2:19	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO 19731	Digital analytics and web analyses for purposes of market, opinion and social research – Vocabularyand service requirements — First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO 28500:2017	Information anddocumentation – WARC file format
ISO/IEC 38500:2015	Information technology – Governance of IT for the organization
ISO/IEC 38505-1:2017	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to thegovernance of data
CAN/CIOSC 100-n	Series of standards for datagovernance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
n/a	DCAM: The Data Management Capability Assessment Model
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
ISO/IEC/IEEE 42020:2019(E)	ISO/IEC/IEEE International Standard – Software, systems and enterprise – Architecture processes
ISO/IEC/IEEE 24765:2017	ISO/IEC/IEEE International Standard – Systems and software engineering – Vocabulary
CSA T100**	ICT Code for Buildings
CSA T200**	Evaluation of software development and cybersecurity programs (update to CSA EXP 200)
CSA EXP 200	Evaluation of software development and cybersecurity programs
CSA T2000-1**	Intelligent Building System Objective Code
CSA T2000-2**	Intelligent Building System Safety Management System Code
CSA Z246.1	Security management for petroleum and natural gas industry systems
CSA N290.7	Cyber security for nuclear power plants andsmall reactor facilities
CSA T150**	Connected and automated vehicle code
CSA T710**	Smart manufacturing readiness assessment methodology and requirements
Z1635**	Canadian Paramedic Information System
CSA Z8000	Canadian health care facilities

۵-۳-۱-۶- استانداردهای مبانی حکمرانی داده _ موضوع ۶: حریم خصوصی (تلقیق شده با موضوع حقوق داده‌ها)

Issue 6 — Data Privacy (consolidated with Issue: Data rights)	
ANSI X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys UsingDiscrete Logarithm Cryptography
ANSI X9.63	Public Key Cryptography for the Financial Services Industry Key Agreement and Key Transport UsingElliptic Curve Cryptography
ANSI X9.73	Cryptographic Message Syntax – ASN.1 and XML – ASCX9
ANSI X9.84	Biometric Information Management and Security for theFinancial Services Industry
ANSI INCITS 446	Information Technology – Identifying Attributes for Named Physical and Cultural Geographic Features(Except Roads and Highways) of the United States, Territories, Outlying Areas, and Freely Associated Areas, and the Waters of the Same to the Limit of the Twelve-Mile Statutory Zone
ASA S12.70	American National Standard Criteria for Evaluating Speech Privacy in Healthcare Facilities
ASCE GSP 226	Geotechnical Engineering State of the Art and Practice Keynote Lectures from GeoCongress 2012
ASTM E2369	Standard Specification for Continuity of Care Record (CCR)
ASTM E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
ASTM E2468	Standard Practice for Metadata to Support Archived Data Management Systems
ASTM E2259 REV A	Standard Guide for Archiving and Retrieving Intelligent Transportation Systems-Generated Data
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
CEN EN 14302	Health informatics – Framework for security requirements for intermittently connected devices
CEN EN 12924	Medical informatics – Security Categorisation and Protection for Healthcare Information Systems
CEN EN 13608-3	Health informatics – Security for healthcare communication – Part 3: Secure data channels
CEN/TR 16742	Intelligent transport systems – Privacy aspects inITS standards and systems inEurope
CEN EN 15969-1	Tanks for transport of dangerous goods – Digital interface for the data transfer between tank vehicleand with stationary facilities – Part 1: Protocol specification – Control, measurement and event data
CEN EN 15969-2	Tanks for transport of dangerous goods – Digital interface for the data transfer between tank vehicleand with stationary facilities – Part 2: Commercial and logistic data
CEN EN 13032-1	Light and lighting — Measurement and presentation of photometric data of lamps and luminaires —Part 1: Measurement and file format – Incorporates Amendment A1: 2012
CEN/TS 15430-2	Winter and road service area maintenance equipment – Data acquisition and transmission – Part 2:Protocol for data transfer between information supplier and client application server
CEN EN 13757-7	Communication systems for meters – Part 7: Transport and security services

CENELEC EN 50491-11	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 11: Smart Metering – Application Specifications – Simple External Consumer Display
CGSB CAN/CGSB-133.1-2017	Security officers and security officer supervisors
CAN/CIOSC 109-1	Qualification and proficiency of privacy and access control professionals
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
CLSI M39-A4	Analysis and Presentation of Cumulative Antimicrobial Susceptibility Test Data; Approved Guideline –Fourth Edition; Vol. 34; No. 2
CLSI AUTO10-A	Autoverification of Clinical Laboratory Test Results; Approved Guideline – First Edition; Vol 26; No 32
CLSI MM20-A	Quality Management for Molecular Genetic Testing; Approved Guideline – Vol 32; No 15
CSA Q830	Model Code for the Protection of Personal Information
CSA B480-02	Customer Service Standard for People with Disabilities – First Edition
CSA B480-02 LARGEPRINT	Customer Service Standard for People with Disabilities – First Edition
CSA CAN/ CSA-B651.2-07	Accessible design for self-service interactive devices – First Edition
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ETSI TR 102 612	Human Factors (HF); European accessibility requirements for public procurement of products and services in the ICT domain (European Commission Mandate M 376, Phase 1) – V1.1.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TR 101 584	Machine-to-Machine Communications (M2M); Study on Semantic support for M2M Data
ETSI EN 300 392-1 V1.6.1	Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI GS INS 002	Identity and Access Management for Networks and Services Distributed Access Control for Telecommunications Use Cases and Requirements – V1.1.1
ETSI TR 102 764	eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth — V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 133 501	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.4.0 Release 16)
IEC 62443-4-2	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

IEC 61158-4-2	Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocolspecification — Type 2 elements
IEC 61158-4-25	Industrial communication networks – Fieldbus specifications – Part 4-25: Data-link layer protocolspecification — Type 25 elements
IEC TS 63134	Active assisted living (AAL) use cases
IEEE 1888 SERIES	Ubiquitous Green Community Control Network Protocol – Includes IEEE 1888; IEEE 1888.1; IEEE 1888.2;IEEE 1888.3; IEEE 1888.4
IEEE 802.1AE	Local and Metropolitan Area Networks – Media Access Control (MAC) Security – IEEE ComputerSociety
IEEE 2410	Biometric Open Protocol
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 802.17	Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 17: Resilient packet ring (RPR) access methodand physical layer specifications — IEEE Computer Society
IES LM-63	APPROVED METHOD: IES STANDARD FILE FORMAT FOR THE ELECTRONIC TRANSFER OFPHOTOMETRIC DATA AND RELATED INFORMATION
ISO 11577	Information technology – Open Systems Interconnection – Network layer security protocol
ISO 18185-4	Freight containers – Electronic seals – Part 4: Data protection
ISO 20215	Space data and information transfer systems – CCSDS cryptographic algorithms – First Edition
ISO 21091	Health informatics – Directory services for healthcare providers, subjects of care and other entities
ISO 21324	Space data and information transfer systems – Space data link security protocol – First Edition
ISO 21549-2	Health informatics – Patient healthcard data– Part 2: Common objects (ISO 21549-2:2014); Englishversion EN ISO 21549-2:2014
ISO 21549-3	Health informatics – Patient healthcard data – Part 3: Limited clinical data (ISO 21549-3:2014); Englishversion EN ISO 21549-3:2014
ISO 21549-4	Health informatics – Patient healthcard data – Part 4: Extended clinical data (ISO 21549-4:2014);English version EN ISO 21549-4:2014
ISO 21549-5	Health informatics – Patient healthcard data – Part 5: Identification data
ISO 21549-6	Health informatics – Patient healthcard data – Part 6: Administrative data
ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002 (ISO27799:2016)
ISO/IEC 10116	Information technology – Security techniques – Modes of operation for an n-bit block cipher
ISO/IEC 10181-5-00	Information technology – Open Systems Interconnection – Security frameworks for open systems:Confidentiality framework
ISO/IEC 11577-97	Information technology – Open Systems Interconnection – Network layer security protocol
ISO/IEC 19772	Information technology – Security techniques – Authenticated encryption
ISO/IEC 19794-11	Information technology – Biometric data interchange formats – Part 11: Signature/sign processeddynamic data
ISO/IEC 19794-13	Information technology – Biometric data interchange formats – Part 13: Voice data

ISO/IEC 19794-7	Information technology – Biometric data interchange formats – Part 7: Signature/sign time series data
ISO/IEC 24713-2	Information technology – Biometric profiles for interoperability and data interchange – Part 2: Physicalaccess control for employees at airports
ISO/IEC 29150/	Information technology – Security techniques – Signcryption
ISO/IEC 30107-2	Information technology – Biometric presentation attack detection – Part 2: Data formats
ISO/IEC/IEEE 18883	Information technology – Ubiquitous green community control network – Security
ISO 10781	Health Informatics – HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM) –Second Edition
ISO TS 27790	Health informatics – Document registry framework – First Edition
ISO 20078-3	Road vehicles – Extended vehicle (ExVe) web services – Part 3: Security
ISO TR 12859	Intelligent transport systems – System architecture – Privacy aspects in ITS standards and systems –First Edition
ISO 12855	Electronic fee collection – Information exchange between service provision and toll charging
ISO 13399-1	Cutting tool data representation and exchange – Part 1: Overview, fundamental principles and generalinformation model
ISO 18440	Space data and information transfer systems – Space link extension – Internet protocol for transferservice — Second Edition
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO 20208	Space data and information transfer systems – Delta-DOR Raw Data Exchange Format – First Edition
ISO 21076	Space data and information transfer systems – Space communications cross support – Architecturerequirements document — First Edition
ISO 22663	Space data and information transfer systems — Proximity-1 space link protocol — Data link layer — Third Edition
ISO/IEC 17417	Information technology – Telecommunications and information exchange between systems – ShortDistance Visible Light Communication (SDVLC) – First Edition
ISO/IEC 20248	Information technology – Automatic identification and data capture techniques – Data structures –Digital signature meta structure – First Edition
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition
ISO TS 22220	Health informatics – Identification of subjects of health care – Second Edition
ISO/IEC 13871-97	Information technology – Telecommunications and information exchange between systems – Privatetelecommunications networks – Digital channel aggregation
ISO/IEC 9798-6	Information technology – Security techniques – Entity authentication – Part 6: Mechanisms usingmanual data transfer
ISO/TS 22220	Health informatics – Identification of subjects of health care
ISO/IEC/IEEE 8802-3	Information technology – Telecommunications and information exchange between systems – Localand metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet
ISO 15396	Space data and information transfer systems – Cross support reference model – Space link extensionservices
ISO 18750	Intelligent transport systems – Co-operative ITS – Local dynamic map (ISO 18750:2018)

ISO 23354	Business requirements for end-to-end visibility of logistics flow – First edition
ISO/IEC 24761:20	Information technology – Security techniques – Authentication context for biometrics
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing
ISO/TR 23786	Road vehicles – Solutions for remote access to vehicle – Criteria for risk assessment
ISO/TR 23791	Road vehicles – Extended vehicle (ExVe) web services – Result of the riskassessment on ISO 20078series
ISO/TS 18750	Intelligent transport systems – Cooperative systems – Definition of a global concept for LocalDynamic Maps (ISO/TS 18750:2015); English version CEN ISO/TS 18750:2015
ISO/IEC 27034-6	Information technology – Security techniques – Application security – Part 6: Case studies
ISO 22857	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal healthdata — Second Edition
ISO/IEC 15944-12	Information technology — Business operational view — Part 12: Privacy protection requirements (PPR)on information life cycle management (ILCM) and EDI of personal information (PI) — First edition
ISO TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment — First Edition
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment – CORR: February 28, 2014
ISO TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information — First Edition
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ITU-T G.9961	Unified high-speed wireline-based home networking transceivers – Data link layer specification –Study Group 15
ITU-T Y.4468	Minimum set of data transfer protocol for automotive emergency response system – Study Group 20
ITU-T Q.1229	Intelligent Network User's Guide for Capability Set 2 – Series Q: Switching and Signalling – IntelligentNetwork — Study Group 11; 175pp
ITU-T Y.3509	Cloud computing – Functional architecture for data storage federation – Study Group 13
ITU-T SERIES Q SUPP 30	Supplement to ITU-T Recommendation Q.1701 – Roadmap to IMT-2000 Recommendations,Standards and Technical Specifications – Study Group 11
ITU-T SERIES Y SUPP 30	ITU-T Y.4250 series – Smart sustainable cities – Overview of smart sustainable cities infrastructure –Study Group 20
ITU-T X.1642	Guidelines for the operational security of cloud computing — Study Group 17
ITU-T Y.1311.1	Network-Based IP VPN Over MPLS Architecture Series Y: Global Information Infrastructure andInternet Protocol Aspects Internet Protocol Aspects – Transport – Study Group 13

ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
SAE AIR6904	Rationale, Considerations, and Framework for Data Interoperability for Health Management within the Aerospace Ecosystem
SAE ARP4294	Data Formats and Practices for Life Cycle Cost Information
SAE GEIA-HB-0007-B	(R) Logistics Product Data Handbook – Formerly TechAmerica SAE GEIA-HB-0007-B
UL 2196	UL Standard for Safety Fire Test for Circuit Integrity of Fire-Resistive Power, Instrumentation, Control and Data Cables – Second Edition; Reprint with revisions through and including November 30, 2018

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
IEEE P7002	Data Privacy
DIACC PCTF 04	Pan-Canadian Trust Framework (PCTF) Privacy: Component Overview and Conformance Profile v1.0
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent: Component Overview and Conformance Profile v1.0
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
CAN/CIOSC 109-1	Qualification and proficiency of privacy and access control professionals
ISO/IEC 27400	Cybersecurity – IoT security and privacy – Guidelines
ISO/IEC 27402	Cybersecurity – IoT security and privacy – Device baseline requirements
ISO/IEC 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
CSA T100**	ICT Code for Buildings
CSA T200**	Evaluation of software development and cybersecurity programs (update to CSA EXP 200)
CSA EXP 200	Evaluation of software development and cybersecurity programs
CSA T2000-1**	Intelligent Building System Objective Code
CSA T2000-2**	Intelligent Building System Safety Management System Code
CSA Z246.1	Security management for petroleum and natural gas industry systems
CSA N290.7	Cyber security for nuclear power plants and small reactor facilities
CSA T150**	Connected and automated vehicle code
CSA T710**	Smart manufacturing readiness assessment methodology and requirements

CAN/CSA-ISO 14971	Medical Devices – Application of Risk Management to Medical Devices
CAN/CSA-CEI/IEC 62304	Medical device software – Software life cycle processes

۵-۳-۱-۷- استانداردهای مبانی حکمرانی داده _ موضوع ۷: راهنمایی بر استفاده قابل اعتماد، اخلاقی و اجتماعی از داده‌ها

Issue 7 — Guidance on trustworthiness, ethical and societal use of data	
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO 10711	Intelligent Transport Systems – Interface Protocol and MessageSet Definition between Traffic SignalControllers and Detectors
ISO 12655	Energy performance of buildings – Presentation of measured energy use of buildings
ISO 13790	Energy performance of buildings – Calculation of energy use for space heating and cooling
ISO TR 17755	Fire safety – Overview of national fire statistics practices – First Edition
ISO TS 14048	Environmental Management – Life Cycle Assessment – Data Documentation Format – First Edition
ISO/IEC 19795-1	Information technology – Biometric performance testing and reporting – Part 1: Principlesand framework
ISO/IEC 29155-1	Systems and software engineering – Information technology project performance benchmarkingframework – Part 1: Concepts and definitions
ISO/IEC 29155-4	Systems and software engineering – Information technology project performance benchmarkingframework Part 4: Guidance for data collection and maintenance
ISO/TS 14048	Environmental management – Life cycle assessment – Data documentation format
ASTM E2129	Standard Practice for Data Collection for Sustainability Assessment of Building Products
ASTM E2166	Standard Practice for Organizing and Managing Building Data
ASTM E2797	Standard Practice for Building Energy Performance Assessment for a Building Involved in a RealEstate Transaction
DIN SPEC 91367	Urban mobility data collection for real-time applications; Text in English
ETSI GS OSG 001	Open Smart Grid Protocol (OSGP) – V1.1.1
IEEE 1616	Motor Vehicle Event Data Recorders (MVEDRs)
IEEE 1856	Framework for Prognostics and Health Management of Electronic Systems
ITU-R RS.1859	Use of remote sensing systems for data collection to be used in the event of natural disasters andsimilar emergencies
ITU-R SA.1164-4	Sharing and coordination criteria for service links in data collection systems using GSO satellites inthe Earth exploration-satellite and meteorological-satellite services
ITU-R SA.1627	Telecommunication requirements and characteristics of EESS and MetSat service systems for datacollection and platform location – Question ITU-R 142/7
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing — Study Group 17
ITU-T Y.3603	Big data – Requirements and conceptual model of metadata for data catalogue – Study

	Group 13
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
CEN 16234-1	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in allsectors — Part 1: Framework
CEN 17161	Design for All – Accessibility following a Design for All approach in products, goods and services –Extending the range of users
ISO 26000	Guidance on social responsibility (ISO 26000:2010)
ISO/IEC TR 29196	Guidance for biometric enrolment
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap Part 2: Architectural componentsand maturity model
ISO/TR 16982	Ergonomics of human-system interaction – Usability methods supporting human-centered design
ISO/TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TR 22758	Biotechnology – Biobanking – Implementation guide for ISO 20387
ISO/TS 14265	Health Informatics – Classification of purposes for processing personal health information
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information
ISO/TS 22220	Health informatics – Identification of subjects of health care
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems onHuman Well-Being
DS DS/CWA 17145-1	Ethics assessment for research and innovation – Part 1: Ethics committee
GOST K32095	Analysing Design Thinking: Studies of Cross-Cultural Co-Creation
CLSI I/LA21-A2	Clinical Evaluation of Immunoassays; Approved Guideline – Second Edition; Vol. 28 No. 22
BSI BS 42020	Biodiversity – Code of practice for planning and development
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and information services
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach – CORR:May 30, 2018
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CLSI H26-A2	Validation, Verification, and Quality Assurance of Automated Hematology Analyzers; ApprovedStandard – Second Edition; Vol 30; No 14
ITU-T SERIES Y SUPP 45	ITU-T Y.4000 series – Smart sustainable cities – An overview of smart sustainable cities and the roleof information and communication technologies – Study Group 20
DS DS-håndbog 107.2	Quality management and quality management systems – Part 2: The “ISO 9000 family”
CEN/TR 15592	Health services – Quality management systems – Guide for the use of EN ISO 9004:2000 in healthservices for performance improvement
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC38500 to the governance of data – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
IEEE 7000 Series	Model Process for Addressing Ethical Concerns During System Design
IEEE P2840	Standard for Responsible AI Licensing

۵-۳-۱-۸- استانداردهای مبانی حکمرانی داده _ موضوع ۸: هماهنگی و قابلیت همکاری اقدامات داده/ داده باز

Issue 8 — Harmonization and interoperability of data practices/ open data	
ISO 5479	Statistical Interpretation of Data – Tests for Departure from the Normal Distribution – First Edition
ISO/IEC 9646-3	Information technology – Open Systems Interconnection (OSI) – Conformance testing methodologyand framework – Part 3: The Tree and Tabular Combined Notation (TTCN)
ISO/IEC TR 10171	Information technology – Telecommunications and information exchange between systems – List ofstandard data link layer protocols that utilize high-level data link control (HDLC) classes of procedures,list of standard XID format identifiers, list of standard mode-setting information field format identifiers,and list of standard user-defined parameter set identification values
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information
ISO/IEC 20016-1	Information technology for learning, education and training – Language accessibility and human interface equivalencies (HIEs) in e-learning applications – Part 1: Framework and reference model forsemantic interoperability
ITU-T H.812	Interoperability design guidelines for personal connected health systems: Services interface –Study Group 16
ITU-T H.830.1	Conformance of ITU-T H.810 personal health system: Services interface Part 1: Web servicesinteroperability: Health & Fitness Service sender — Study Group 16
ITU-T H.830.10	Conformance of ITU-T H.810 personal health system: Services interface Part 10: hData ObservationUpload: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.11	Conformance of ITU-T H.810 personal health system: Services interface Part 11: Questionnaires: Health& Fitness Service sender — Study Group 16

ITU-T H.830.12	Conformance of ITU-T H.810 personal health system: Services interface Part 12: Questionnaires: Health& Fitness Service receiver — Study Group 16
ITU-T H.830.13	Conformance of ITU-T H.810 personal health system: Services interface Part 13: Capability Exchange:Health & Fitness Service sender — Study Group 16
ITU-T H.830.14	Conformance of ITU-T H.810 personal health system: Services interface Part 14: Capability Exchange:Health & Fitness Service receiver — Study Group 16
ITU-T H.830.15	Conformance of ITU-T H.810 personal health system: Services interface Part 15: FHIR ObservationUpload: Health & Fitness Service sender – Study Group 16
ITU-T H.830.16	Conformance of ITU-T H.810 personal health system: Services interface Part 16: FHIR ObservationUpload: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.2	Conformance of ITU-T H.810 personal health system: Services interface Part 2: Web servicesinteroperability: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.4	Conformance of ITU-T H.810 personal health system: Services interface Part 4: SOAP/ATNA: Health &Fitness Service receiver — Study Group 16
ITU-T H.830.5	Conformance of ITU-T H.810 personal health system: Services interface Part 5: PCD-01 HL7messages: Health & Fitness Service sender – Study Group 16
ITU-T H.830.7	Conformance of ITU-T H.810 personal health system: Services interface Part 7: Consent management:Health & Fitness Service sender – Study Group 16
ITU-T H.830.8	Conformance of ITU-T H.810 personal health system: Services interface Part 8: Consent Management:Health & Fitness Service receiver – Study Group 16
ITU-T H.830.9	Conformance of ITU-T H.810 personal health system: Services interface Part 9: hData ObservationUpload: Health & Fitness Service sender – Study Group 16
ITU-T H.831	Conformance of ITU-T H.810 personal health devices: WAN interface Part 1: Web servicesinteroperability: Sender – Study Group 16
ITU-T H.832	Conformance of ITU-T H.810 personal health devices: WAN interface Part 2: Web servicesinteroperability: Receiver – Study Group 16
ITU-T H.834	Conformance of ITU-T H.810 personal health devices: WAN interface Part 4: SOAP/ATNA: Receiver –Study Group 16
ITU-T H.835	Conformance of ITU-T H.810 personal health devices: WAN interface Part 5: PCD-01 HL7 messages:Sender — Study Group 16
ITU-T H.836	Conformance of ITU-T H.810 personal health devices: WAN interface Part 6: PCD-01 HL7 messages:Receiver — Study Group 16
ITU-T H.837	Conformance of ITU-T H.810 personal health devices: WAN interface Part 7: Consent management:Sender — Study Group 16
ITU-T H.838	Conformance of ITU-T H.810 personal health devices: WAN interface Part 8: Consent Management:Receiver — Study Group 16
ITU-T Q.3954	oneM2M – Interoperability testing – Study Group 20
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC38500 to the governance of data – First Edition

ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TR 38502	Information technology – Governance of IT – Framework and model
ISO/IEC TR 38504	Governance of information technology – Guidance for principles-based standards in the governanceof information technology
ISO/IEC TS 38501	Information technology – Governance of IT – Implementation guide
SNZ AS/NZS 8016	Governance of IT enabled projects
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/IEC 27560	Privacy technologies – Consent record information structure
ISO/IEC 38505-1:2017	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC38500 to the governance of data
N/A	Joint Initiative for Global Standards Harmonization Health Informatics Document Registry and Glossary
N/A	New European Interoperability Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 103-4	Digital trust and identity – Part 4: Digital wallets
IEEE 1900.6-2011	IEEE Standard for Spectrum Sensing Interfaces and Data Structures for Dynamic Spectrum Accessand other Advanced Radio Communication Systems
IEEE P2896	Standard for Open Data: Open Data Ontology
IEEE P1484.11.1	Standard for Learning Technology – Data Model for Content Object Communication
IEEE 1609.11-2010	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Over-the-Air ElectronicPayment Data Exchange Protocol for Intelligent Transportation Systems (ITS)
IEEE C37.118.2-2011	IEEE Standard for Synchrophasor Data Transfer for Power Systems
IEEE/IEC C37.111-2013	IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems
IEEE 1451.0-2007	IEEE Standard for a Smart Transducer Interface for Sensors and Actuators – Common Functions,Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats
IEEE 2418.2-2020	IEEE Standard for Data Format for Blockchain Systems
N/A	Statistics Canada Statistical Standards (Concepts, Classifications, and Variables)
N/A	Data Documentation Initiative (DDI) – The Data Documentation Initiative (DDI) is an international standard for describing the data produced by surveys and other observational methods in the social,behavioral, economic, and health sciences. Standards include, XKOS, DDI Lifecycle, DDI-Codebook and DDI-CDI
N/A	Data Catalog Vocabulary (DCAT) – An RDF vocabulary designed to facilitate interoperability betweendata catalogs

۵-۳-۱-۹- استانداردهای مبانی حکمرانی داده _ موضوع ۹: بازیگران داده و نقش‌های تراکنش‌های داده

Issue 9 — Data actor and data transaction roles	
CEN EN 13608-3	Health informatics – Security for healthcare communication – Part 3: Secure data channels
SNZ AS/NZS 5478	Recordkeeping metadata property reference set (RMPRS)
CEN/TR 15449-3	Geographic information – Spatial data infrastructures – Part 3: Data centric view
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing — Study Group 17
ITU-T X.1641	Guidelines for doud service customer data security — Study Group17
ISO 16175.1	Information and documentation-Principles and functional requirements for records in electronic officeenvironments Part 1: Overview and statement of principles
ISO 16175-1	Information and documentation – Principles and functional requirements for records in electronicoffice environments – Part 1: Overview and statement of principles
ASTM D4840	Standard Guide for Sample Chain-of-Custody Procedures
ASTM E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
ETSI TS 187 001	Network Technologies (NTECH); NGN SECurity (SEC); Requirements – V3.9.1
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
ISO/TS 8000-150	Data quality – Part 150: Master data: Quality management framework

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
N/A	EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation(EU) 2018/1725
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
IEEE 117-2015	IEEE Standard Test Procedure for Evaluation of Systems of Insulating Materials for Random-WoundAC Electric Machinery
IEEE P2957	Standard for aReference Architecture for Big Data Governance and Metadata Management
IEEE P802.3cy	Standard for Ethernet Amendment: Physical Layer Specifications and Management Parameters forgreater than 10 Gb/s Electrical Automotive Ethernet

IEEE 1588-2019	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement andControl Systems
IEEE P2144.2	This standard defines the functional requirements in data compliance, governance and risk management in the operational process for Blockchain-based IoT data management systems
IEEE P802.1CBcv	Draft Standard for Localand metropolitan area networks – Frame Replication and Elimination for Reliability Amendment: Information Model, YANG Data Model and Management InformationBase Module
IEEE P2418.2	The standard establishes data format requirements for a blockchain system (s).

۵-۳-۱-۱۰- استانداردهای مبانی حکمرانی داده _ موضوع ۱۰: کاربردهای (ثانوی از) داده‌ها

Issue 10 — Secondary use of data

DS DS/CWA 17145-1	Ethics assessment for research and innovation – Part 1: Ethics committee
ISO/IEC 29184	Information technology – Online privacy notices and consent – First edition
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2:Reference architecture and requirements
CSA CSA-Q830-03	Model Code for the Protection of Personal Information – Second Edition
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
DS DS/CWA 14355	Guidelines for the implementation of Secure Signature-Creation Devices
ETSI TR 102 458	Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US FederalBridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456) – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
IEC 61970-405	Energy management system application program interface (EMS-API) – Part 405: Generic Eventingand Subscription (GES)
IEC 62541-8	OPC unified architecture – Part 8: Data access – Edition 3.0
ISO 19115.1	Geographic information-Metadata Part 1: Fundamentals – Incorporating Amendment No. 1: June 2018
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO 19132	Geographic information – Locationbased services – Reference model
ISO/IEC 7816-11	Identification cards – Integrated circuit cards – Part 11: Personal verification through biometricmethods - Second Edition
ISO/IEC TR 24729-4	Information technology – Radio frequency identification for item management – Implementationguidelines – Part 4: Tag data security – First Edition
ISO/IEC 24791-5	Information technology – Radio frequency identification (RFID) for item management – Softwaresystem infrastructure – Part 5: Device interface
ISO/IEC 9579-04	Information technology – Remote database access for SQL with security enhancement
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ETSI TS 102 342	Digital Enhanced Cordless Telecommunications (DECT); Cordless multimedia communication system;Open Data Access Profile (ODAP) — V1.2.1

ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
ETSI TS 183 064	Telecommunications and Internet converged Services and Protocols for Advanced Networking(TISPAN); NGN integrated IPTV subsystem stage 3 specification – V3.4.1; Includes Diskette
IEEE 1619.2	Wide-Block Encryption for Shared Storage Media – IEEE Computer Society
IEC 62628	Guidance on software aspects ofdependability — Edition 1.0
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability – First Edition
ISO/IEC 25024	Systems and software engineering – Systems and software Quality Requirements and Evaluation(SQuaRE) — Measurement of data quality
IEEE 1232.1	Trial Use – Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE): Data and Knowledge Specification
IEEE STDVA24228	BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP
ITU-T X.1602	Security requirements for software as aservice application environments — Study Group 17
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derivedrequirements — First Edition
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use — First Edition
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/IEC TS 19249	Information technology – Security techniques – Catalogue of architectural and design principles forsecure products, systems and applications
ISO/IEC 23751	Information technology – Cloud computing and distributed platforms – Data sharing agreement (DSA)framework
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use
ISO 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO 26000	Guidance on social responsibility

IWA 26:2017	Using ISO 26000:2010 in management systems
IWA 27 – sharing economy (TC 324)	Guiding principles and framework for the sharing economy
ISO/AWI 31700	Consumer protection – Privacy by design for consumer goods and services
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
IEEE P2933	Standard for clinical IoT Data & Devices interoperability with TIPPSS
IEEE P2876	Recommended Practice for Inclusion, Dignity and Privacy in Online Gaming
IEEE P7002	Data Privacy Process
IEEE P7012	Standard for Machine Readable Personal Privacy Terms
IEEE 2410	IEEE Standard for Biometric Open Protocol
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent: Component Overview and ConformanceProfile v1.0

۵-۳-۲- استانداردهای مرتبط با کارگروه ۲: جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها

۵-۳-۲-۱- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع ۱۱: جمع‌آوری (گردآوری) داده‌ها

Issue 11 — Data Collection	
NSC 120810000	Safety Metrics
ISO/TS 14048	Environmental Management – Life Cycle Assessment – Data Documentation Format – First Edition
ITU-R SA.1627	Telecommunication requirements and characteristics of EESS and MetSat service systems for datacollection and platform location – Question ITU-R 142/7
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model
ITU-T SERIES Y SUPP 50	ITU-T Y.3650-series – Use case and application scenario for big-data-driven networking –Study Group 13
ITU-T Y.2618	The M interface in public packet telecommunication data networks – Study Group 13
ITU-T Y.2619	Operation, administration and maintenance functions and mechanisms for the public packettelecommunication data network (PTDN) – Study Group 13
ITU-T Y.2620	T interface for the public packet telecommunication data network – Study Group 13
ITU-T Y.3071	Data aware networking (information centric networking) – Requirements and capabilities – StudyGroup 13
ITU-T Y.3174	Framework for data handling to enable machine learning in future networks including IMT-2020 –Study Group 13

ITU-T Y.3505	Cloud computing – Overview and functional requirements for data storage federation –Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ITU-T Y.3604	Big data – Overview and requirements for data preservation – Study Group 13
ITU-T Y.3650	Framework of big-data-driven networking – Study Group 13
ITU-T Y.3651	Big-data-driven networking – mobile network traffic management and planning – Study Group 13
ITU-T Y.4461	Framework of open data in smart cities – Study Group 20
ITU-T Y.4468	Minimum set of data transfer protocol for automotive emergency response system – Study Group 20
ITU-T Y.4467	Minimum set of data structure for automotive emergency response system – Study Group 20
ITU-T SERIES Y SUPP 40	Big data standardization roadmap – Study Group 13
ITU-T SERIES Y SUPP 48	Proof-of-concept for data service using information centric networking in IMT-2020 – Study Group 13
ISO/IEC 29161	Information technology – Data structure – Unique identification for the Internet of Things –First Edition
ITU-T Y.2068	Functional framework and capabilities of the Internet of things – Study Group 13
ITU-T Y.3603	Big data – Requirements and conceptual model of metadata for data catalogue – Study Group 13
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ISO/IEC 23006-4	Information technology – Multimedia service platform technologies – Part 4: Elementary services –Second Edition
DS DS/CWA 16385	Interoperability of Registries
ISO/IEC 12034-1	Information technology – Archive eXchange Format (AXF) – Part 1: Structure and semantics –First Edition
BSI BS 17898	Code of practice for the management of observed hydrometric data
ISO/IEC 12785-2	Information technology – Learning, education, and training – Content packaging – Part 2: XMLbinding — First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-	Data governance – Part 1: Data protection of digital assets

1:2020	
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CSA Z8003	Health care design research and evaluation

۵-۳-۲-۲- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع ۱۲: مدیریت سیستم‌های داده

Issue 12 — Data systems management	
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
ETSI GS ZSM 002	Zero-touch network and Service Management (ZSM); Reference Architecture – V1.1.1
ISO 37156	Smart community infrastructures – Guidelines on data exchange and sharing for smart communityinfrastructures
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO/IEC 27034-3	Information technology – Application security Part 3: Application security management process
ITU-T M.3041	Framework of smart operation, management and maintenance – Study Group 2
ITU-T M.3363	Requirements for data management in the telecommunication management network – Study Group 2
ITU-T Y.3604	Big data – Overview and requirements for data preservation – Study Group 13
IEC 62974-1	Monitoring and measuring systems used for data collection, gathering and analysis – Part 1:Device requirements
ISO/IEC 29155-4	Systems and software engineering – Information technology project performance benchmarkingframework Part 4: Guidance for data collection and maintenance
ISO 26162	Systems to manage terminology, knowledge and content – Design, implementation and maintenanceof terminology management systems
SAE GEIA-859A	Data Management – Formerly TechAmerica GEIA-859 REV A
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
SAE GEIA-HB-859	Implementation Guide for Data Management – Formerly TechAmerica GEIA-HB-859
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing – First Edition
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ISO/IEC TR 10032	Information technology – Reference Model of Data Management
ISO/IEC 10164-2	Information technology — Open Systems Interconnection — Systems Management: State Management Function AMENDMENT 1 : Implementation conformance statement proformasTECHNICAL CORRIGENDUM 1 – First Edition

ASTM E2842	Standard Guide for Credentialing for Access to an Incident or Event Site
ISO/IEC 10164-1	Information Technology – Open Systems Interconnection – Systems Management: ObjectManagement Function – First Edition; Amendment: 5/15/1996; Corrigendum: 12/15/1996

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data

۵-۳-۲-۳- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع۱۳: قابلیت کشف داده‌ها

Issue 13 — Discoverability of the data	
ANSI INCITS 284	Information Technology – Identification Cards – Health Care Identification Cards
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
IEC 62541-8	OPC unified architecture – Part 8: Data Access
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 24091	Information technology – Power efficiency measurement specification for data center storage –First edition
ISO/IEC 7816-11	Identification cards – Integrated circuit cards – Part 11: Personal verification through biometricmethods — Second Edition
ISO/IEC 9579-04	Information technology – Remote database access for SQL with security enhancement
ISO/TR 17424	Intelligent transport systems – Cooperative systems – State of the art of Local Dynamic Maps concepts
ISO 19115.1	Geographic information-Metadata Part 1: Fundamentals – Incorporating Amendment No. 1: June 2018
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
IEC TS 61850-7-7	Communication networks and systems for power utility automation — Part 7-7: Machine-processableformat of IEC 61850-related data models for tools — Edition 1.0
ISO/IEEE 11073-10101	Health informatics — Point-of-care medical device communication — Part 10101: NomenclatureAMENDMENT 1: Additional definitions – First Edition
CLSI AUTO16	Next-Generation In Vitro Diagnostic Instrument Interface – 1st Edition; Volume 39;

	Number 4
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ISO 20078-3	Road vehicles – Extended vehicle (ExVe) web services – Part 3: Security
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
CEN EN 16931-1	Electronic invoicing — Part 1: Semantic data model of thecore elements of an electronic invoice —Incorporates Amendment A1: 2019
DIN CEN/TS 17262	Personal identification – Robustness against biometric presentation attacks – Application to EuropeanAutomated Border Control; English version CEN/TS 17262:2018
DS DS/CEN/TR 16931-4	Electronic invoicing – Part 4: Guidelines on interoperability of electronic invoices at the transmission level
DS DS/CEN/TS 17262	Personal identification – Robustness against biometric presentation attacks – Application to EuropeanAutomated Border Control
ETSI EN 300 175-4	Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data LinkControl (DLC) layer — V2.8.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 102 563	Digital Audio Broadcasting (DAB); DAB+ audio coding (MPEG HE-AACv2) – V2.1.1
ETSI TS 103 466	Digital Audio Broadcasting (DAB); DAB audio coding (MPEG Layer II) – V1.2.1
ISO 17427-1	Intelligent transport systems – Cooperative ITS – Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s) (ISO 17427-1:2018)
ISO 17892-12	Geotechnical investigation and testing — Laboratory testing of soil — Part 12: Determination of liquidand plastic limits (ISO 17892-12:2018)
ISO 18185-4	Freight containers – Electronic seals – Part 4: Data protection
ISO 24534-3	Intelligent transport systems – Automatic vehicle and equipment identification – Electronicregistration identification (ERI) for vehicles – Part 3: Vehicle data – Second Edition
ISO 13527	Space data and information transfer systems – XML formatted data unit (XFDU) structure andconstruction rules — First Edition
ISO 14199	Health informatics – Information models – Biomedical Research Integrated Domain Group(BRIDG) Model
ISO 14825	Intelligent transport systems – Geographic Data Files (GDF) – GDF5.0
ISO 15489-1	Information and documentation – Records management – Part 1: Concepts and principles
ISO 15836-1	Information et documentation — L'ensemble des éléments de métadonnées Dublin Core — Partie 1 : Éléments principaux
ISO 15836-2	Information and documentation – The Dublin Core metadata element set Part 2: DCMI Propertiesand classes
ISO 16684-1	Graphic technology – Extensible metadata platform (XMP) Part 1: Data model, serialization andcore properties
ISO 16684-2	Graphic technology – Extensible metadata platform (XMP) Part 2: Description of XMP schemasusing RELAX NG
ISO 17316	Information and documentation – International standard link identifier (ISLI)
ISO 17972-1	Graphic technology – Colour data exchange format – Part 1: Relationship to CxF3

	(CxF/X)
ISO 17972-2	Graphic technology – Colour data exchange format (CxF/X) – Part 2: Scanner target data (CxF/X-2)
ISO 17972-3	Graphic technology – Colour data exchange format (CxF/X) – Part 3: Output target data (CxF/X-3) –First Edition
ISO 19109	Geographic information – Rules for application schema
ISO 19111	Geographic information – Referencing by coordinates
ISO 19115.2	Geographic information – Metadata Part 2: Extensions for acquisition and processing
ISO 19115-2	Geographic information — Metadata — Part 2 : extensions for acquisition and processing
ISO 19130.2	Geographic information-Imagery sensor models for geopositioning Part 2: SAR, InSAR, lidar and sonar
ISO 19130-1	Geographic information – Imagery sensor models for geopositioning – Part 1: Fundamentals
ISO 19139.2	Geographic information-Metadata – XML schema implementation Part 2: Extensions for imageryand gridded data
ISO 19150-4	Geographic information – Ontology – Part 4: Service ontology
ISO 19159.1	Geographic information – Calibration and validation of remote sensing imagery sensors and data Part1: Optical sensors
ISO 19159.3	Geographic information – Calibration and validation of remote sensing imagery sensors and data Part3: SAR/InSAR
ISO 19160.1	Addressing Part 1: Conceptual model
ISO 19160-1	Addressing – Part 1: Conceptual model
ISO 19162	Geographic information – Well-known text representation of coordinate reference systems
ISO 19165.1	Geographic information – Preservation of digital data and metadata Part 1: Fundamentals
ISO 19165-1	Geographic information – Preservation of digital data and metadata Part 1: Fundamentals
ISO 19289	Air quality – Meteorology – Siting classifications for surface observing stations on land – First Edition
ISO 19445	Graphic technology – Metadata for graphic arts workflow – XMP metadata for image anddocument proofing
ISO 19593-1	Graphic technology – Use of PDF to associate processing steps and content data – Part 1: Processingsteps for packaging and labels
ISO 20614	Information and documentation – Data exchange protocol for interoperability and preservation
ISO 20616-2	Graphic technology – File format for quality control and metadata Part 2: Print Quality eXchange (PQX)
ISO 2108	Information and documentation – International Standard Book Number (ISBN)
ISO 21812-1	Graphic technology – Print product metadata for PDF files Part 1: Architecture and core requirementsfor metadata
ISO 23081-1	Information and documentation – Records management processes – Metadata for records –Part 1 :principles
ISO 24097-1	Intelligent transport systems – Using web services (machine-machine delivery) for ITS servicedelivery – Part 1: Realization of interoperable web services – Second Edition
ISO 24619	Language resource management — Persistent identification and sustainable access

	(PISA) (ISO24619:2011)
ISO 24622-2	Language resource management – Component metadata infrasctructure (CMDI) Part 2: Componentmetadata specification language
ISO 25577	Information and documentation – MarcXchange
ISO 26324	Information and documentation – Digital object identifier system
ISO 27730	Information and documentation – International standard collection identifier (ISCI)
ISO 28258	Soil quality — Digital exchange of soil-related data— Incorporates Amendment A1: 2019
ISO 28500	Information and documentation – WARC file format
ISO 639-4	Codes for the representation of names of languages – Part 4: General principles of coding of therepresentation of names of languages and related entities, and application guidelines
ISO 8	Information and documentation – Presentation and identification of periodicals
ISO TR 13054	Knowledge management of health information standards – First Edition
ISO TR 13128	Health informatics – Clinical document registry federation – First Edition
ISO TR 17321-2	Graphic technology and photography – Colour characterization of digital still cameras (DSCs) – Part 2:Considerations for determining scene analysis transforms – First Edition
ISO TR 23081-3	Information and documentation – Managing metadata for records – Part 3: Self-assessmentmethod — First Edition
ISO TR 24097-2	Intelligent transport systems – Using web services (machine-machine delivery) for ITS servicedelivery – Part 2: Elaboration of interoperable web services' interfaces – First Edition
ISO TR 24097-3	Intelligent transport systems – Using web services (machine-machine delivery) for ITS servicedelivery – Part 3: Quality of service – First Edition
ISO TS 13972	Health informatics – Detailed clinical models, characteristics and processes – First Edition
ISO TS 15926-12	Industrial automation systems and integration — Integration of lifecycle data for process plants including oil and gas production facilities — Part 12: Life-cycle integration ontology represented in WebOntology Language (OWL)
ISO TS 17439	Health informatics – Development of terms and definitions for health informatics glossaries –First Edition
ISO TS 17948	Health informatics – Traditional Chinese medicine literature metadata – First Edition
ISO TS 19115-3	Geographic information – Metadata – Part 3: XML schema implementation for fundamentalconcepts — First Edition
ISO TS 19159-2	Geographic information – Calibration and validation of remote sensing imagery sensors and data –Part 2: Lidar — First Edition
ISO TS 19159-3	Geographic information – Calibration and validation of remote sensing imagery sensors and data –Part 3: SAR/InSAR — First edition
ISO TS 20428	Health informatics – Data elements and their metadata for describing structured clinical genomicsequence information in electronic health records – First Edition
ISO TS 21526	Health informatics – Metadata repository requirements (MetaRep) – First edition
ISO/IEC 11179-1	Information technology – Metadata registries (MDR) – Part 1: Framework – Third Edition
ISO/IEC 11179-5	Information technology – Metadata registries (MDR) – Part 5: Naming principles – Third Edition
ISO/IEC 11179-6	Information technology – Metadata registries (MDR) – Part 6: Registration – Third

	Edition
ISO/IEC 14957	Information technology – Representation of data element values – Notation of the format –Second Edition
ISO/IEC 15444-2	Information technology – JPEG 2000 image coding system: Extensions – Incorporates Corrigendum3: December 2006; Corrigendum 4: December 2010
ISO/IEC 15444-5	Information technology – JPEG 2000 image coding system: Reference software – Second Edition
ISO/IEC 15444-6	Information technology – JPEG 2000 image coding system – Part 6: Compound image file format –Second Edition
ISO/IEC 15444-8	Information technology – JPEG 2000 image coding system – Part 8: Secure JPEG 2000
ISO/IEC 16500-6	Information technology – Generic digital audio-visual systems – Part 6: Information representation
ISO/IEC 19566-5	Information technologies – JPEG systems – Part 5: JPEG universal metadata box format (JUMBF) –First edition
ISO/IEC 19763-5	Information technology – Metamodel framework for interoperability (MFI) – Part 5: Metamodel forprocess model registration — First Edition
ISO/IEC 19763-6	Information technology – Metamodel framework for interoperability (MFI) – Part 6: RegistrySummary — First Edition
ISO/IEC 19788-7	Information technology – Learning, education and training – Metadata for learning resources – Part 7:Bindings — First edition
ISO/IEC 19788-8	Information technology – Learning, education and training – Metadata for learning resources – Part 8:Data elements for MLR records — First Edition
ISO/IEC 19788-9	Information technology – Learning, education and training – Metadata for learning resources – Part 9:Data elements for persons — First Edition
ISO/IEC 19794-13	Information technology – Biometric data interchange formats – Part 13: Voice data – First Edition
ISO/IEC 20248	Information technology – Automatic identification and data capture techniques – Data structures –Digital signature meta structure – First Edition
ISO/IEC 20944-2	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 2: Codingbindings — First Edition
ISO/IEC 20944-3	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 3: APIbindings — First Edition
ISO/IEC 20944-4	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 4: Protocolbindings — First Edition
ISO/IEC 20944-5	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 5:Profiles — First Edition
ISO/IEC 21000-22	Information technology – Multimedia framework (MPEG-21) – Part 22: User Description
ISO/IEC 22602	Informationsteknologi – Lغr ing, uddannelse og trغn ing – Model for kompetencer udtrykt i metadatatil lغri ngsressourcer (MLR)
ISO/IEC 23000-22	Information technology – Multimedia application format (MPEG-A) – Part 22: Multi-image applicationformat (MIAF) — First edition
ISO/IEC 23001-10	Information technology – MPEG systems technologies – Part 10: Carriage of timed metadata metricsof media in ISO base media file format – Second edition
ISO/IEC 23001-11	Information technology – MPEG systems technologies – Part 11: Energy-efficient media consumption(green metadata) — Second edition
ISO/IEC 23001-13	First edition

ISO/IEC 23001-7	Information technology – MPEG systems technologies – Part 7: Common encryption in ISO basemedia file format files — Third Edition
ISO/IEC 23005-4	Information technology – Media context and control – Part 4: Virtual world object characteristics –Fourth Edition
ISO/IEC 23008-12	Information technology — High efficiency coding and media delivery in heterogeneous environments —Part 12: Image File Format — First Edition
ISO/IEC 23008-3	Information technology – High efficiency coding and media delivery in heterogeneous environments –Part 3: 3D audio AMENDMENT 1: Audio metadata enhancements – Second edition
ISO/IEC 23092-3	Information technology – Genomic information representation – Part 3: Metadata and applicationprogramming interfaces (APIs) – First edition
ISO/IEC 24800-5	Information technology – JPSearch – Part 5: Data interchange format between image repositories –First Edition
ISO/IEC 29500-2	Information technology – Document description and processing languages – Office Open XML FileFormats – Part 2: Open Packaging Conventions – Third Edition
ISO/IEC 40260	Information technology — W3C Web Services Addressing 1.0 — Metadata — First Edition; IncludesAccess to Additional Content
ISO/IEC TR 11179-2	Information technology – Metadata registries (MDR) – Part 2: Classification – First edition
ISO/IEC TR 15938-11	Information technology – Multimedia content description Interface – Part 11: MPEG-7 profile schemas
ISO/IEC TR 15938-8	Information technology – Multimedia content description interface – Part 8: Extraction and use ofMPEG-7 descriptions
ISO/IEC TR 19583-1	Information technology – Concepts and usage of metadata – Part 1: Metadata concepts –First edition
ISO/IEC TR 19583-22	Information technology – Concepts and usage of metadata – Part 22: Registering and mappingdevelopment processes using ISO/IEC 19763 – First Edition
ISO/IEC TR 20943-1	Information technology Procedures for achieving metadata registry (MDR) content consistency Part 1:Data elements — First Edition
ISO/IEC TR 20943-3	Information technology Procedures for achieving metadata registry content consistency Part 3: Valuedomains — First Edition
ISO/IEC TR 20943-5	Information technology – Procedures for achieving metadata registry content consistency – Part 5:Metadata mapping procedure – First Edition
ISO/IEC TR 20943-6	Information technology – Procedures for achieving metadata registry content consistency – Part 6:Framework for generating ontologies – First Edition
ISO/IEC TR 21000-11	Information technology – Multimedia framework (MPEG-21) – Part 11: Evaluation Tools for PersistentAssociation Technologies
ISO/IEC TS 11179-30	Information technology – Metadata registries (MDR) – Part 30: Basic attributes of metadata –First edition
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems,software, and services information – First Edition
ISO/TR 23081-3	Information and documentation. Managing metadata for records. Self-assessment method – Hardcopy Only – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
ISO/TS 19115-3	Geographic information – Metadata Part 3: XML schema implementation for fundamental concepts
ISO/TS 19130	Geographic information – Imagery sensor models for geopositioning
ISO/TS 19130-2	Geographic information – Imagery sensor models for geopositioning – Part 2: SAR,

	InSAR, lidarand sonar
ISO/TS 19139	Geographic information – Metadata – XML schema implementation
ISO/TS 19139-2	Geographic information – Metadata – XML schema implementation Part 2: Extensions for imageryand gridded data
ITU-R BS.2076-2	Audio Definition Model
ITU-R BS.2088-1	Long-form file format for the international exchange of audio programme materials with metadata
ITU-T F.750	Metadata framework
ITU-T T.804	Information technology – JPEG 2000 image coding system: Reference software – Study Group 16
ITU-T T.805	(Pre-Published) Information technology – JPEG 2000 image coding system: Compound imagefile format
ITU-T T.808	Information technology – JPEG 2000 image coding system: Interactivity tools, APIs and protocols
ITU-T X.1276	Authentication step-up protocol and metadata Version 1.0 — Study Group 17
ITU-T Y.3603	Big data – Requirements and conceptual model of metadata for data catalogue – Study Group 13
ULC CAN/ULC-S316-14	STANDARD FOR PERFORMANCE OF VIDEO SURVEILLANCE SYSTEMS – First Edition
ISO/IEC TR 29163-1	Information technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition –Part 1: Overview Version 1.1 — Third edition
ITU-T X.1255	Framework for discovery of identity management information — Study Group 17
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derivedrequirements — First Edition
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
ISO/IEC TR 29163-2	Information technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition –Part 2: Content Aggregation Model Version 1.1 – Third Edition
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services
ISO/IEC 30141	Internet of Things (loT) – Reference Architecture
ISO/IEC 30118-2	Information technology – Open Connectivity Foundation (OCF) Specification Part 2: Security specification
ISO/IEC 23271	Information technology Common Language Infrastructure – Adopted by INCITS
ISO/IEC 30118-1	Information technology – Open Connectivity Foundation (OCF) Specification Part 1: Core specification
ISO 16175.2	Information and documentation – Principles and functional requirements for records in electronic office environments Part 2: Guidelines and functional requirements for digital recordsmanagement systems
ISO 16175-2	Information and documentation – Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for digital recordsmanagement systems
ISO/IEC 23270	Information technology C# Language Specification – Adopted by INCITS
ISO/IEC 19763-1	Information technology – Metamodel framework for interoperability (MFI) – Part 1: Framework
ANSI INCITS 530	Information Technology – Architecture for Managed Computing Systems
ISO/IEC 18384-1	Information technology – Reference Architecture for Service Oriented Architecture (SOA RA) Part 1:Terminology and concepts for SOA

ISO/IEC TR 30102	Information technology – Distributed Application Platforms and Services (DAPS) – General technicalprinciples of Service Oriented Architecture
ISO/IEC TR 22417	Information technology – Internet of things (IOT) – IOT use cases
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach – CORR:May 30, 2018
ISO/IEC 23271	Information technology – Common Language Infrastructure (CLI) – Third Edition
IEC 62656-1	Standardized product ontology register and transfer by spreadsheets — Part 1: Logical structure fordata parcels — Edition 1.0
IEC 82045-1	Document Management — Part 1: Principles and Methods — Edition 1.0
ISO 19115	Geographic information Metadata
ISO/IEC 11179-3	Information technology – Metadata registries (MDR) – Part 3: Registry metamodel and basicattributes — Third Edition
ISO/IEC 20802-1	Information technology – Open dataprotocol (OData) v4.0 Part 1: Core – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CIOSC/PAS 100-4:2020	Data governance – Part 4: Specification for Scalable Remote Access Infrastructure
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 106-1	Discovery and management of Digital Twins for built environments – Part 1: Discovery
IEEE 1667-2018	IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices
IEEE P2957	Standard for a Reference Architecture for Big Data Governance and Metadata Management
IEEE P1951.1	Standard for Smart City Component Systems Discovery and Semantic Exchange of Objectives
IEEE P1752	IEEE Approved Draft Standard for Mobile Health Data
N/A	Statistics Canada Statistical Standards (Concepts, Classifications, and Variables)
N/A	Data Documentation Initiative (DDI) – The Data Documentation Initiative (DDI) is an international standardfor describing the dataproduced by surveys and other observational methods in the social, behavioral,economic, and health sciences. Standards include, XKOS, DDI Lifecycle, DDI-Codebook and DDI-CDI
N/A	Data Catalog Vocabulary (DCAT) – An RDF vocabulary designed to facilitate interoperability betweendata catalogs

۵-۳-۲-۴- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع۱۴: پیوند(لینک کردن) داده‌ها

Issue 14 _ Data Linkage	
API BULL 1178	Integrity Data Management and Integration – FIRST EDITION
ETSI TR 103 290	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment – V1.1.1
ETSI TR 103 376	SmartM2M; IoT LSP use cases and standards gaps – V1.1.1
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existingstandardized IoT Platforms — V1.1.2
ETSI TS 118 101	Functional Architecture – V2.10.0; oneM2M TS-0001 version 2.10.0 Release 2
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information
ISO TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations –First Edition
ISO 22857	Health informatics – Guidelines on data protection to facilitate transborder flows of personal health data
ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002 (ISO27799:2016)
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use — First Edition
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derivedrequirements — First Edition
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability – First Edition
ISO/IEC 20006.1	Information technology for learning, education and training – Information model for competency Part1: Competency general framework and information model
ISO/IEC 20006-1	Information technology for learning, education and training – Information model for competency –Part 1: Competency general framework and information model – First Edition
ISO/IEC 21823-1	Internet of things (IoT) – Interoperability for iot systems Part 1: Framework
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TR 20547-5	Information technology – Big data reference architecture – Part 5: Standards roadmap – First edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TS 19763-13	Information technology – Metamodel framework for interoperability (MFI) – Part 13: Metamodel forform design registration — First Edition
ISO/IEC/IEEE 24748-7	Systems and software engineering – Life cycle management Part 7: Application of systemsengineering on defense programs
ITU-T X.1363	(Pre-Published) Technical framework of personally identifiable information (PII) handling in Internetof things (IoT) environment

ITU-T X.1040	Security reference architecture for lifecycle management of e-commerce business data —Study Group 17
ITU-T SERIES Y SUPP 40	Big data standardization roadmap – Study Group 13
ITU-T X.814	Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems:Confidentiality Framework – Data Networks and Open System Communications Security 25 pp
ITU-T Y.4203	Requirements of things description in the Internet of things – Study Group 20
ITU-T Z.100 ANNEX F1	Specification and Description Language — Overview of SDL-2010 Annex F1: SDL-2010 formal definition:General overview — Study Group 17
ITU-T Z.100 ANNEX F3	Specification and Description Language — Overview of SDL-2010 Annex F3: SDL-2010 formaldefinition: Dynamic semantics — Study Group 17

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
IEEE Std 1888.4-2016	IEEE Standard for Green Smart Home and Residential Quarter Control Network Protocol –
IEEE P2030	IEEE Guide for Smart Grid Interoperability of Energy Technology and Information TechnologyOperation with the Electric Power System (EPS), End-
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework

۵-۳-۲-۵- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع۱۵: برچسب‌گذاری دستی داده‌ها

Issue 15 — Manual tagging of data	
ISO/IEC 19790	Information technology – Security techniques – Security requirements for cryptographic modules –Second Edition; Corrected version 12/15/2015
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operationalenvironment — First Edition
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
BSI BS 5701-2	Guide to quality control and performance improvement using qualitative (attribute) data – Part 2:Fundamentals of standard attribute charting for monitoring, control and improvement
ISO 19731	Digital analytics and web analyses for purposes of market, opinion and social research – Vocabularyand service requirements — First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada

۵-۳-۲-۶- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع ۱۶: مدیریت متادیتا

Issue 16 — Metadata management	
ISO/IEC 23001-13	Information technology – MPEG systems technologies – Part 13: Media orchestration
IEC 82045-1	Document Management — Part 1: Principles and Methods — Edition 1.0
IEC 82045-2	Document management – Part 2: Metadata elements and information reference model
IEEE 1484.12.3	Standard for Learning Technology – Extensible Markup Language (XML) Schema Definition LanguageBinding for Learning Object Metadata – IEEE Computer Society
IEEE COMP	IEEE Standard Computer Dictionary Compilation of IEEE Standard Computer Glossaries – IEEEComputer Society Document
ISO 17369	Statistical data and metadata exchange (SDMX) – First Edition
ISO 24622-1	Language resource management – Component Metadata Infrastructure (CMDI) Part 1: TheComponent Metadata Model
BIS IS 15992	Information and Documentation – The Dublin Core Metadata Element Set
ISO 15836	Information and documentation – The Dublin Core metadata element set TECHNICAL CORRIGENDUM1 — Second Edition
ISO 15836-1	Information and documentation – The Dublin Core metadata element set – Part 1: Core elements –First Edition
ISO 15836-2	Information and documentation – The Dublin Core metadata element set – Part 2: DCMI Propertiesand classes — First edition
SNZ SA/SNZ HB 168	Document control
ISO/IEC 11179-1	Information technology – Metadata registries (MDR) – Part 1: Framework – Third Edition
ISO 24622-2	Language resource management – Component metadata infrasctructure (CMDI) – Part 2:Component metadata specification language – First edition
IEEE STDVA24228	BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP
ISO/IEC 11179-6	Information technology – Information technology – Metadata registries (MDR) – Part 6: Registration
ETSI GR NFV-SEC 003	Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance – V1.2.1
ASTM E2468	Standard Practice for Metadata to Support Archived Data Management Systems
ISO/IEC TR 20943-6	Information technology – Procedures for achieving metadata registry content consistency – Part 6:Framework for generating ontologies – First Edition
ISO/IEC 11179-2	Information technology Metadata registries (MDR) Part 2: Classification – Second Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
IEEE P2957	Standard for aReference Architecture for Big Data Governance and Metadata Management
IEEE P2881	Standard for Learning Metadata
IEEE P4002	Standard for Synthetic Aperture Radar Metadata Content
IEEE P4003	IEEE Draft Standard for Global Navigation Satellite System-Reflectometry (GNSS-R) Data andMetadata Content
IEEE IC17-006	Big Data Governance and Metadata Management
N/A	Statistics Canada Statistical Standards (Concepts, Classifications, and Variables)
N/A	Data Documentation Initiative (DDI) – The Data Documentation Initiative (DDI) is an international standardfor describing the dataproduced by surveys and other observational methods in the social, behavioral,economic, and health sciences. Standards include, XKOS, DDI Lifecycle, DDI-Codebook and DDI-CDI
N/A	Data Catalog Vocabulary (DCAT) – An RDF vocabulary designed to facilitate interoperability betweendata catalogs

۵-۳-۲-۷- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع۱۷: استراتژی‌های خط‌مشی داده‌های سازمانی و مدیریت مخاطره (ریسک)

Issue 17 —Organizational Data policy strategies and risks management	
ANSI X9.111	Penetration Testing within the Financial Services Industry – ASCX9
ANSI X9.100-181	Specification for TIFF Image Format for Image Exchange
API BULL 1178	Integrity Data Management and Integration – FIRST EDITION
API PUBL 353	Managing Systems Integrity of Terminal and Tank Facilities Managing the Risk of Liquid PetroleumReleases — First Edition
API PUBL 4620	International Oil Spill Conference Proceedings Achieving and Maintaining Preparedness
ASCE GSP 98	PAVEMENT SUBGRADE, UNBOUND MATERIALS, AND NONDESTRUCTIVE TESTING
ASHRAE HVAC APPLICATIONS SI HANDBOOK	2019 ASHRAE Handbook HVAC Applications SI Edition
ASTM MNL19	Manual on the Building of Materials Databases
ASTM E2842	Standard Guide for Credentialing for Access to an Incident or Event Site
ASTM F3286	Standard Guide for Cybersecurity and Cyberattack Mitigation
ASTM F3449	Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems inAccordance with IMO Resolution MSC.428(98) – Cyber Risks and Challenges
ASTM E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)
ASTM E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems

ASTM MNL58	Petroleum Refining and Natural Gas Processing
AWWA G410	Business Practices for Operation and Management
BSI BS 70000	Medical physics, clinical engineering and associated scientific services in healthcare – Requirementsfor quality, safety and competence
BSI PD 7506	Linking Knowledge Management with other Organizational Functions and Disciplines: A Guide toGood Practice
BSI PD 8100	Smart cities overview – Guide
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code ofpractice for implementation of BS 10008-1
BSI PD 7505	Skills for Knowledge Working: A Guide to Good Practice
BSI PAS 197	Code of practice for cultural collections management
CEN/TR 15584	Characterisation of sludges – Guide to risk assessment especially in relation to use and disposalof sludges
CEN 17255-2	Stationary source emissions – Data acquisition and handling systems – Part 2: Specification ofrequirements on data acquisition and handling systems
CEN/TR 17370	Public transport – Operating raw data and statistics exchange
CEN/TS 17434	Ambient air – Determination of the particle number size distribution of atmospheric aerosol using aMobility Particle Size Spectrometer (MPSS)
CEN EN 50518	Monitoring and Alarm Receiving Centre
CEN/TR 16674	Information technology – Analysis of privacy impact assessment methodologies relevant to RFID
CENELEC EN 50436-6	Alcohol interlocks – Test methods and performance requirements – Part 6 : data security
CENELEC EN 50491-12-1	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Smart grid – Application specification – Interface and framework forcustomer — Part 12-1: Interface between the CEM and Home/Building Resource manager — General Requirements and Architecture
CENELEC EN 50600-3-1	Information technology – Data centre facilities and infrastructures – Part 3-1: Management andoperational information
CLSI QMS22	Management of Paper-based and Electronic Laboratory Information – First Edition
DS DS/CWA 15847	Innovation, Coordination and Collaboration in Service Driven Manufacturing Supply Chains –Reference Model for Industrial Services
ETSI TS 187 001	Network Technologies (NTECH); NGN SECurity (SEC); Requirements – V3.9.1
ETSI GS ISI 002	Information Security Indicators (ISI); Event Model A security event classification model andtaxonomy — V1.2.1
ETSI TR 102 659-1	GRID; Study of ICT Grid interoperability gaps; Part 1: Inventory of ICT Stakeholders – V1.2.1
GOST R 34.13	Information technology. Cryptographic data security. Block ciphers operation modes

IEC 62056-21	Electricity Metering — Data Exchange for Meter Reading, Tariff and Load Control — Part 21: Direct LocalData Exchange — Edition 1.0
IEC 62962	Particular requirements for load-shedding equipment (LSE)
IEC/IEEE 82079-1	Preparation ofinformation for use (instructions for use) of products – Part 1: Principles and generalrequirements — Edition 2.0
IEC 62443-2-1	Industrial communication networks — Network and system security — Part 2-1: Establishing an industrial automation and control system security program – First Edition
IEC 60300-3-15	Dependability management Part 3-15: Application guide – Engineering of system dependability
IEEE 1232.1	Trial Use – Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE): Data and Knowledge Specification
IEEE 1685	IP-XACT, Standard Structure for Packaging, Integrating, and Reusing IP within Tool Flows – IEEEComputer Society
IEEE 1455	Standard for Message Sets for Vehicle/Roadside Communications
IEEE 1484.11.2	Learning Technology – ECMAScript Application Programming Interface for Content to RuntimeServices Communication – IEEE Computer Society
IEEE 1914.1	Packet-based Fronthaul Transport Network – Includes Access to Additional Content
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE ICICLE	IEEE IC INDUSTRY CONSORTIUM ON LEARNING ENGINEERING
ISO 8000-2	Data quality Part 2: Vocabulary
ISO/TS 8000-65	Data quality – Part 65: Data quality management: Process measurement questionnaire
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO/IEC 20547-3	Information technology – Big data reference architecture – Part 3: Reference architecture – First edition
ISO/IEC 38506	Information technology – Governance of IT – Application of ISO/IEC 38500 to the governance of ITenabled investments — First edition
ISO 14644-2	Cleanrooms and associated controlled environments – Part 2: Monitoring to provide evidence ofcleanroom performance related to air cleanliness by particle concentration
ISO 14031	Environmental Management – Environmental Performance Evaluation – Guidelines
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 13211-1	Information technology – Programming languages – Prolog – Part 1: General core
ISO/IEC 19778-1	Information technology – Learning, education and training – Collaborative technology – Collaborativeworkplace – Part 1: Collaborative workplace data model

ISO/IEC 9075-2	Information technology – Database languages – SQL – Part 2: Foundation (SQL/Foundation) –Fifth Edition
ISO/IEC TS 18508	Information technology – Additional Parallel Features in Fortran – First Edition
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition
ISO 17427-1	Intelligent transport systems – Cooperative ITS – Part 1: Roles and responsibilities in the context ofco-operative ITS architecture(s) (ISO 17427-1:2018)
ISO 17892-12	Geotechnical investigation and testing — Laboratory testing of soil — Part 12: Determination of liquidand plastic limits (ISO 17892-12:2018)
ISO TR 23791	Road vehicles – Extended vehicle (ExVe) web services – Result of the risk assessment on ISO 20078series — First edition
ISO/TS 17427	Intelligent transport systems – Cooperative systems – Roles and responsibilities in the context ofcooperative ITS based on architecture(s) for cooperative systems
ISO 15638-21	Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 21: Monitoring of regulated vehicles using roadside sensorsand data collected from the vehicle for enforcement and other purposes
ISO/IEC TR 24729-4	Information technology – Radio frequency identification for item management – Implementationguidelines – Part 4: Tag data security – First Edition
ISO 16598	Timber structures – Structural classification for sawn timber – First Edition
ISO TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles –First Edition
ISO 16919	Space data and information transfer systems – Requirements for bodies providing audit andcertification of candidate trustworthy digital repositories – First Edition
ISO 22307	Financial services – Privacy impact assessment
ISO/IEC TS 33072	Information technology – Process assessment – Process capability assessment model forinformation security management
ISO/TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls(ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)
ISO/IEC 15504-6	Information technology – Process assessment – Part 6: An exemplar system life cycle processassessment model — First Edition
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles
ISO/HL7 27951 cd-rom	Health informatics – Common terminology services, release 1
ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy informationmanagement – Requirements and guidelines
ISO/IEC 27018	Information technology – Security techniques – Code of practice for protection of personallyidentifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27017	Information technology – Security techniques – Code of practice for information security controlsbased on ISO/IEC 27002 for cloud services

ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiableinformation protection
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation ofvirtualized servers — First Edition
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO 41001	Facility management – Management systems – Requirements with guidance for use – First Edition
ISO 30302	Information and documentation – Management systems for recordkeeping-Guidelinesfor implementation
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information — First Edition
ITU-T Y.2330	Requirements of next generation network evolution for supporting freedata service – Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T X.1040	Security reference architecture for lifecycle management of e-commerce business data —Study Group 17
ITU-T X.1086	Telebiometrics protection procedures – Part 1: A guideline to technical and managerialcountermeasures for biometric data security – Study Group 17
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing — Study Group 17
ITU-T X.1641	Guidelines for doud service customer data security — Study Group17
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
NEMA MITA CSP 1	Cybersecurity for Medical Imaging
NEN NPR-CR 1832	CIM Systems Architecture – Enterprise model execution and integration services – Statementof requirements
SAE GEIA-859A	Data Management – Formerly TechAmerica GEIA-859 REV A
SAE GEIA-HB-649A	(R) Configuration Management Standard Implementation Guide
SAE GEIA-HB-859	Implementation Guide for Data Management – Formerly TechAmerica GEIA-HB-859
SAE PT-182	Integrated Vehicle Health Management – System of Systems Integration – To PurchaseCall 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide

SNV SN CR 13694	Health informatics – Safety and Security Related Software Quality Standards for Healthcare (SSQS)
SNZ NZS 8153	Health Records
SNZ SA/SNZ HB 168	Document control

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
IEEE/ISO/IEC 29119-2-2013	ISO/IEC/IEEE International Standard – Software and systems engineering – Software testing –Part 2:Test processes
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data deidentification framework
n/a	Best Practice Guide to Applying Data Sharing Principles
CAN/CIOSC 100-n	Series of standards for datagovernance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data

۵-۳-۲-۸- استانداردهای جمع‌آوری، سازماندهی و درجه‌بندی داده‌ها _ موضوع۱۸: ارزیابی کیفیت و تناسب داده‌ها برای استفاده (کاربرد)

Issue 18 — Data Quality and Fitness for Use Assessment	
ISO/TS 8000-1	Data quality – Part 1: Overview
ISO/TS 8000-110	Data quality — Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, andconformance to data specification
ISO TS 8000-311	Data quality – Part 311: Guidance for the application of product data quality for shape (PDQ-S) –First Edition
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO TS 8000-1	Data quality – Part 1: Overview – First Edition; Includes Access to Additional Content
ISO 8000-8	Data quality Part 8: Information and data quality: Concepts and measuring
ISO 17369	Statistical data and metadata exchange (SDMX) – First Edition
API BULL 1178	Integrity Data Management and Integration – FIRST EDITION
ISO/TS 14048-03	Environmental management – Life cycle assessment – Data documentation format – First Edition

ISO 8000-100	Data quality – Part 100: Master data: Exchange of characteristic data: Overview – First Edition
ISO/IEC 25012	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Dataquality model — First Edition
ISO 8000-140	Data quality – Part 140: Master data: Exchange of characteristic data: Completeness – First Edition
ISO 8000-110	Data quality — Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, andconformance to data specification — First Edition; Includes Access to Additional Content
ISO 8000-130	Data quality – Part 130: Master data: Exchange of characteristic data: Accuracy – First Edition
ISO 8000-116	Data quality Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 toauthoritative legal entity identifiers
ISO 8000-2	Data quality – Part 2: Vocabulary – Third Edition
ISO/TS 8000-150	Data quality – Part 150: Master data: Quality management framework
ISO 8000-62	Data quality – Part 62: Data quality management: Organizational process maturity assessment:Application of standards relating to process assessment – First Edition
ISO 8000-120	Data quality – Part 120: Master data: Exchange of characteristic data: Provenance – First Edition
ISO 8000-63	Data quality Part 63: Data quality management: Process measurement
ISO/IEC 25020	Systems and software engineering – Systems and software Quality Requirements and Evaluation(SQuaRE) – Quality measurement framework – Second edition
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
CEN 16991	Risk-based inspection framework – CORR: August 31, 2018
IEC 31010	Risk management – Risk assessment techniques
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/IEC/IEEE 26511	Systems and software engineering – Requirements for managers of information for users of systems,software, and services
ISO/TS 8000-65	Data quality – Part 65: Data quality management: Process measurement questionnaire
ISO/TS 9002	Quality management systems – Guidelines for the application ofISO 9001:2015 – CORR:November 30, 2016
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO TS 8000-60	Data quality – Part 60: Data quality management: Overview – First Edition
ISO 8000-115	Data quality – Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolutionrequirements — First Edition
ISO/IEC TR 12382	Permuted Index of the Vocabulary of Information Technology – Second Edition
ISO 19115.1	Geographic information-Metadata Part 1: Fundamentals – Incorporating Amendment No. 1: June 2018
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO TR 14873	Information and documentation – Statistics and quality issues for web archiving – First Edition
ITU-T E.840	Statistical framework for end-to-end network performance benchmark scoring and ranking — StudyGroup 12

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
ISO 25000 series	SQuaRE (System and Software Quality Requirements and Evaluation)
ISO 25012	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Dataquality model
ISO 8000 series	Data Quality and Enterprise Master Data
n/a	FAIR Principles
n/a	Statistics Canada's Quality Assurance Framework
n/a	Statistics Canada's Quality Assurance Framework
n/a	Statistics Canada's Data Quality Toolkit
IEEE P2896	Standard for Open Data: Open Data Ontology
IEEE P2957	Standard for aReference Architecture for Big Data Governance and Metadata Management
IEEE P2963	Data Formats for Smart Legal Contracts
IEEE P2975	Standard for Industrial Artificial Intelligence (AI) Data Attributes
IEEE P3205	Standard for Blockchain Interoperability – Data Authentication and Communication Protocol
IEEE P3803	Standard for Household Appliance Customer Data Assetization and Commercialization Requirements

۵-۳-۳- استانداردهای مرتبط با کارگروه ۳: دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها

۵-۳-۳-۱- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع۱۹: مدیریت رضایت (رضایت، دسترسی و برداشت از داده‌ها)

Issue 19 — Consent Management (Consent, Access and Withdrawal to Data)	
BSI BS 10012	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 8611	Robots and robotic devices Guide to the ethical design and application of robots and robotic systems
BSI PAS 1192-5	Specification for security-minded building information modelling, digital built environments and smartasset management
BSI PD CEN/TS 16685	Information technology – Notification of RFID – The information sign to be displayed in areas whereRFID interrogators are deployed
BSI PD CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
CEN EN 14484	Health informatics – International transfer of personal health data covered by the EU data protectiondirective – High level security policy; German version EN 14484:2003, text in English
CEN EN 14485	Health informatics – Guidance for handling personal health data in international applications in thecontext of the EU data protection directive
CEN EN 14822-2	Health informatics – General purpose information components – Part 2: Non-clinical; Englishversion EN 14822-2:2005
CEN EN 15224	Quality management systems – EN ISO 9001:2015 for healthcare
CEN/TR 15300	Health Informatics – Framework for formal modelling of healthcare security policies
CEN/TR 16674	Information technology – Analysis of privacy impact assessment methodologies relevant to RFID
CEN/TS 15480-4	Identification card systems – European Citizen Card – Part 4: Recommendations for European CitizenCard issuance, operation and use
CEN-EN 16571	Information technology – RFID privacy impact assessment process
CLSI HS1-A2	A Quality Management System Model for Health Care;Approved Guideline – Second Edition;Vol 24; No 37
CLSI QMS01-A4	Quality Management System: AModel for Laboratory Services; Approved Guideline — Fourth Edition;Vol 31; No 15
CLSI QMS22	Management of Paper-based and Electronic Laboratory Information – First Edition
CSA CAN/CSA-C22.2NO. 60950-23-07	Information Technology Equipment – Safety – Part 23: Large Data Storage Equipment – First Edition
CSA CAN/ CSA-Z900.2.1-17	Tissues for assisted reproduction – Third Edition
CSA CSA Z710:15	Métis Nation Registry Operations – First Edition
CSA CSA-Q830-03	Model Code for the Protection of Personal Information – Second Edition
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
CSA Z316.7-12	Primary sample collection facilities and medical laboratories – Patient safety and

	quality of care –Requirements for collecting, transporting, and storing samples – First Edition
CSA Z8000-18	Canadian health care facilities – Second Edition
DS DS/CWA 50487	SmartHouse Code ofPractice
ETSI EG 202 487	Human Factors (HF); User experience guidelines; Telecare services (eHealth) – V1.1.2
ETSI GS INS 009	Identity and access management for Networks and Services (INS); Security and privacy requirementsfor collaborative cross domain network monitoring – V1.1.1
ETSI GS ISI 002	Information Security Indicators (ISI); Event Model A security event classification model andtaxonomy — V1.2.1
ETSI GS ISI 005	Information Security Indicators (ISI); Guidelines for security eventdetection testing and assessment ofdetection effectiveness — V1.1.1
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A ConcreteApproach — V1.1.1
ETSI TR 102 688-8	Media Content Distribution (MCD); MCD framework; Part 8: Audience Measurement – V1.1.1
ETSI TR 102 935	Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart GridNetworks; Impact of Smart Grids on M2M platform – V2.1.1
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TR 118 516	oneM2M; Study of Authorization Architecture for Supporting Heterogeneous Access ControlPolicies – V2.0.0; oneM2M TR-0016 version 2.0.0
IEEE 1735	Recommended Practice for Encryption and Management of Electronic Design Intellectual Property(IP) – IEEE Computer Society; Incorporating Corrigendum 1: 2015
ISO 10781	Health Informatics – HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM)
ISO 22600-3	Health informatics – Privilege management and access control – Part 3: Implementations (ISO22600-3:2014)
ISO 22857	Health informatics – Guidelines on data protection to facilitate transborder flows of personalhealth data
ISO 5127	Information and documentation – Foundation and vocabulary
ISO 8000-100	Data quality – Part 100: Master data: Exchange of characteristic data: Overview
ISO 8000-120	Data quality – Part 120: Master data: Exchange of characteristic data: Provenance
ISO 8000-130	Data quality – Part 130: Master data: Exchange of characteristic data: Accuracy
ISO 8000-140	Data quality – Part 140: Master data: Exchange ofcharacteristic data: Completeness
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO 834-2	Fire-resistance tests – Elements of building construction Part 2: Requirements and recommendationsfor measuring furnace exposure on test samples
ISO HL7 21731	Health informatics HL7 version 3 Reference information model Release 1 – First Edition; CorrectedVersion 10/15/2012
ISO TR 11636	Health Informatics – Dynamic on-demand virtual private network for health informationinfrastructure — First Edition
ISO TS 20658	Medical laboratories – Requirements for collection, transport, receipt, and handling of

	samples –First Edition
ISO TS 27790	Health informatics – Document registry framework – First Edition
ISO TS 29585	Health informatics – Deployment of a clinical data warehouse – First Edition
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
ISO/IEC 10181-3	Information technology – Open Systems Interconnection – Security frameworks for open systems –Part 3: Access control framework
ISO/IEC 10746-2	Information technology – Open distributed processing – Reference model: Foundations
ISO/IEC 10779	Information technology – Office equipment – Accessibility guidelines for older persons and personswith disabilities
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 24745	Information technology – Security techniques – Biometric information protection
ISO/IEC 29100	Information technology – Security techniques – Privacy framework – AMD: July 31, 2018
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment – CORR:April 30, 2020
ISO/IEC 29146	Information technology – Security techniques – A framework for access management
ISO/IEC 29187-1	Information technology – Identification of privacy protection requirements pertaining to learning,education and training (LET) – Part 1: Framework and reference model – First Edition
ISO/IEC TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commercialapplications – Part 1: General guidance (Technical Report)
ISO/IEC TR 24729-4	Information technology – Radio frequency identification for item management – Implementationguidelines — Tag data security
ISO/IEC TR 24772	Information technology – Programming languages – Guidance to avoiding vulnerabilities inprogramming languages through language selection and use
ISO/TR 17791	Health informatics – Guidance on standards for enabling safety in health software
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 14265	Health informatics – Classification of purposes for processing personal health information – CORR:March 31, 2014
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment – CORR: February 28, 2014
ISO/TS 19475-2	Document management – Minimum requirements for the storage of documents Part 2: Storage
ISO/TS 20658	Medical laboratories – Requirements for collection, transport, receipt, and handling of samples
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles
ISO/TS 22600-3	Health informatics – Privilege management and access control – Part 3: Implementations
ISO/TS 27790	Health informatics – Document registry framework
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse

ANSI AARST MS-QA	Radon Measurement Systems Quality Assurance
ISO/IEC 29190:18	Information technology – Security techniques – Privacy capability assessment model
ISO/IEC TR 23186:20	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/WD 24366	Natural Persons Identifier
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
IEEE P7002	Data Privacy Process
IEEE P7004	Standard for Child and Student Data Governance
IEEE P7005	IEEE Draft Standard for Transparent Employer Data Governance
IEEE P7006	Standard for Personal Data Artificial Intelligence (AI) Agent
IEEE P7008	Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems
IEEE P7012	Standard for Machine Readable Personal Privacy Terms
IEEE P7014	Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems
IEEE P2089	Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children
IEEE P3800	Standard for a data-trading system: overview, terminology and reference model
IEEE P2895	Standard Taxonomy for Responsible Trading of Human-Generated Data
IEEE IC16-002	The Global Initiative on Ethics of Autonomous and Intelligent Systems
IEEE IC17-002	Digital Inclusion, Identity, Trust, and Agency
IEEE IC19-004	Technology and Data Harmonization for Enabling Clinical Decentralized Clinical Trials
IEEE IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

۵-۳-۳-۲- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۰: دسترسی به داده‌ها

Issue 20- Data Access	
BSI BS 10102-2	Big data Part 2: Guidance ondata-intensive projects
ISO 23081-2	Information and documentation – Managing metadata for records – Part 2: Conceptual andimplementation issues
ISO/IEC 13522-6	Information Technology – Coding of Multimedia and Hypermedia Information – Part 6: Support forEnhanced Interactive Applications
ISO/IEC 27002	Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27040	Information technology – Security techniques – Storage security (ISO/IEC 27040:2015)
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29146	Information technology – Security techniques – A framework for access management – First Edition
ISO/IEC TR 30166	Internet of Things (IoT) – Industrial IoT
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
IEEE P2975	Standard for Industrial Artificial Intelligence (AI) Data Attributes
CSA Z8003	Health care design research and evaluation

۵-۳-۳-۳- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۱: نگهداری داده‌ها

Issue 21 — Data retention	
CEN EN 14484	Health informatics – International transfer of personal health data covered by the EU data protectiondirective – High level security policy; German version EN 14484:2003, text in English
ANSI INCITS 306	Information Technology – SCSI-3 Block Commands (SBC)
ANSI INCITS 516	Information Technology – SCSI Stream Commands – 4 (SSC-4)
ANSI X9.129	Legal Orders Exchange – Version 02
ANSI X9.84	Biometric Information Management and Security for theFinancial Services Industry
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code ofpractice for implementation of BS 10008-1
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and information services
BSI PAS 1885	The fundamental principles of automotive cyber security – Specification

CEN EN 14485	Health informatics – Guidance for handling personal health data in international applications in thecontext of the EU data protection directive; German version EN 14485:2003, text in English
CEN EN 16072	Intelligent transport systems – ESafety – Pan-European eCall operating requirements
CEN EN 16571	Information technology – RFID privacy impact assessment process
CEN/TR 16673	Information technology – RFID privacy impact assessment analysis for specific sectors
CEN/TR 16674	Information technology – Analysis of privacy impact assessment methodologies relevant to RFID
CEN/TR 16742	Intelligent transport systems – Privacy aspects inITS standards and systems inEurope
CEN/TS 15480-4	Identification card systems – European Citizen Card – Part 4: Recommendations for European CitizenCard issuance, operation and use
CENELEC CEN/CLC/ ETSI/TR 50572	Functional reference architecture for communications in smart metering systems
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
DS DS/CWA 17356	Interoperability of security systems for the surveillance of widezones
ETSI EG 202 798	Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperabilitytesting — V1.1.1
ETSI ETR 295	Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); User Requirements forSubscriber Identity Module (SIM)
ETSI GS INS 009	Identity and acess management for Networks and Services (INS); Security and privacy requirementsfor collaborative cross domain network monitoring – V1.1.1
ETSI GS ISI 008	Information Security Indicators (ISI); Description of an Overall Organization-wide Security Informationand Event Management (SIEM) Approach – V1.1.1
ETSI GS MOI 002	Measurement Ontology for IP traffic (MOI); Requirements for IP traffic measurement ontologiesdevelopment — V1.1.1
ETSI GS MOI 003	Measurement Ontology for IP traffic (MOI); IP traffic measurement ontologies architecture – V1.1.1;Includes Diskette
ETSI GS MOI 010	Measurement Ontology for IP traffic (MOI); Report on information models for IP traffic measurement — V1.1.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and RegulatoryConcerns — V1.1.1
ETSI GS NGP 001	Next Generation Protocols (NGP); Scenario Definitions – V1.3.1
ETSI SR 002 298	Response from CEN nd ETSI to the "Communication fromthe Commission tothe Council, theEuropean Parliament, the European Economic and Social Committee and the Committee of theRegions: Network and Information Security: Proposal for a European Policy Approach" – V1.1.1
ETSI SR 002 564	Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth – V2.0.0
ETSI SR 003 392	Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment;A new snapshot of Cloud Computing Standards – V2.1.1
ETSI TR 102 299	Emergency Communications (EMTEL); Collection of European Regulatory Texts and orientations — V1.4.1
ETSI TR 102 438	Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards inEurope — V1.1.1
ETSI TR 102 512	Terrestrial Trunked Radio (TETRA); Security; Security requirements analysis for modulationenhancements to TETRA

ETSI TR 102 725	Machine-to-Machine communications (M2M); Definitions – V1.1.1
ETSI TR 102 762	Human Factors (HF); Intelligent Transport Systems (ITS); ICT in cars – V1.1.1
ETSI TR 103 118	Machine-to-Machine communications (M2M); Smart Energy Infrastructures security; Review ofexisting security measures and convergence investigations – V1.1.1
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 533	SmartM2M; Security; Standards Landscape and best practices – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TS 102 412	Smart Cards; Smart Card Platform Requirements Stage 1 – V12.1.0; Release 12
ETSI TS 102 657	Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery ofretained data — V1.25.1; Includes Diskette
ETSI TS 103 443-2	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition TechnologyEngineering and Operational Aspects; Part 2: NAT64 – V1.1.1
ETSI TS 103 443-3	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition TechnologyEngineering and Operational Aspects; Part 3: DS-Lite – V1.1.1
ETSI TS 103 443-5	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition TechnologyEngineering and Operational Aspects; Part 5: 464XLAT – V1.1.1
ETSI TS 103 443-6	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition TechnologyEngineering and Operational Aspects; Part 6: 6RD – V1.1.1
ETSI TS 105 174-2	Access, Terminals, Transmission and Multiplexing (ATTM); Broadband Deployment and LifecycleResource Management; Part2: ICT Sites: Implementation of energy and lifecycle management practices — V1.3.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
IEC 61360-4	Standard data element types with associated classification scheme for electric components – Part 4:IEC reference collection of standard data element types and component classes
IEC 61512-4	Batch control Part 4: Batch production records
IEC 63119-1	Information exchange for electric vehicle charging roaming service Part 1: General
IEC 82304-1	Health Software – Part 1: General requirements for product safety
IEC TR 80001-2-8	Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified inIEC TR 80001-2-2
IEC/TR 62939-1	Smart grid user interface Part 1: Interface overview and country perspectives
IEC/TR 80001-2-8	Application of risk management for IT-networks incorporating medical devices Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identifiedin IEC TR 80001-2-2
IEEE 2001	Recommended Practice for the InternetWeb Site Engineering, Web Site Management, and Web SiteLife Cycle – IEEE Computer Society Document
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 2755.1	Guide for Taxonomy for Intelligent Process Automation Product Features and Functionality

ISO/IEC 15944-9	Information technology – Business Operational View – Part 9: Business transaction traceabilityframework for commitment exchange
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ISO/IEC 17789:16	Information technology – Cloud computing – Reference architecture
ISO/IEC 18014-4	Information technology – Security techniques – Time-stamping services Part 4: Traceability oftime sources
ISO/IEC 18043	Information technology – Security techniques – Selection, deployment and operations of intrusiondetection systems
ISO/IEC 19086-1	Information technology – Cloud computing – Service level agreement (SLA) framework Part 1:Overview and concepts
ISO/IEC 19086-3	Information technology – Cloud computing – Service level agreement (SLA) framework Part 3: Coreconformance requirements
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security andof protection of PII
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use
ISO/IEC 20748.2	Information technology for learning, education and training – Learning analytics interoperability Part 2:System requirements
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 27004	Information technology – Security techniques – Information security management – Monitoring,measurement, analysis and evaluation
ISO/IEC 27034-5	Information technology – Security techniques – Application security Part 5: Protocols and applicationsecurity controls data structure
ISO/IEC 27037	Information technology – Security techniques – Guidelines for identification, collection, acquisitionand preservation of digital evidence (ISO/IEC 27037:2012)
ISO/IEC 27039	Information technology – Security techniques – Selection, deployment and operations of intrusiondetection systems (IDPS) – CORR: June 30, 2018
ISO/IEC 27040	Information technology – Security techniques – Storage security
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29100	Information technology – Security techniques – Privacy framework – AMD: July 31, 2018
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29110-4-3	Systems and software engineering – Lifecycle profiles for very small entities (VSEs) – Part 4-3:Service delivery – Profile specification – First Edition
ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment –First Edition
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiableinformation protection
ISO/IEC 29155-2	Systems and software engineering – Information technology project performance benchmarkingframework Part 2: Requirements for benchmarking
ISO/IEC 29184	Information technology – Online privacy notices and consent
ISO/IEC 29341-30-1	Information technology – UPnP Device Architecture – Part 30-1: IoT management and control devicecontrol protocol – IoT management and control architecture overview –

	First Edition
ISO/IEC 30137-1	Information technology – Use of biometrics in video surveillance systems Part 1: System designand specification
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC38500 to the governance of data
ISO/IEC TR 15067-3-2	Information technology – Home electronic system application model Part 3-2: GridWise –Interoperability context-setting framework
ISO/IEC TR 15947	Information technology – Security techniques – IT intrusion detection framework
ISO/IEC TR 16166	Information technology – Telecommunications and information exchange between systems – NextGeneration Corporate Networks (NGCN) – Security of session-based communications – First Edition
ISO/IEC TR 20000-9	Information technology – Service management Part 9: Guidance on the application of ISO/IEC20000-1 to cloud services
ISO/IEC TR 20748-2	Information technology for learning, education and training – Learning analytics interoperability Part 2:System requirements – CORR: August 31, 2018
ISO/IEC TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commericalapplications Part 1: General guidance
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 29110-5-3	Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) Part 5-3: Servicedelivery guidelines
ISO/IEC TR 29196	Information technology – Guidance for biometric enrolment
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TS 27034-5-1	Information technology – Application security – Part 5-1: Protocols and application security controlsdata structure, XML schemas
ISO/IEC/IEEE 12207	Systems and software engineering – Software life cycle processes
ISO/IEC/IEEE 15289	Systems and software engineering – Content of life-cycle information items (documentation)
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems,software, and services information
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/IEC/IEEE 29148	Systems and software engineering – Life cycle processes – Requirements engineering
ISO/IEC/IEEE 90003	Software engineering – Guidelines for the application of ISO 9001:2015 to computer software
ISO/TR 10255	Document management applications – Optical disk storage technology, management and standards
ISO/TR 12859	Intelligent transport systems – System architecture – Privacy aspects in ITS standards and systems
ISO/TR 14742	Financial services – Recommendations on cryptographic algorithms and their use
ISO/TR 17427-3	Intelligent transport systems – Cooperative ITS Part 3: Concept of operations (ConOps) for‘core’ systems
ISO/TR 17427-4	Intelligent transport systems – Cooperative ITS Part 4: Minimum system requirements and behaviourfor core systems
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/TR 17797	Electronic archiving – Selection of digital storage media for long term preservation
ISO/TR 80002-2	Medical device software Part 2: Validation of software for medical device quality

	systems
ISO/TS 17427	Intelligent transport systems – Cooperative systems – Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems (ISO/TS 17427:2014); English versionCEN ISO/TS 17427:2014
ISO/TS 19299	Electronic fee collection – Security framework (ISO/TS 19299:2015); English version CEN ISO/TS 19299:2015
ISO/TS 21089	Health informatics – Trusted end-to-end information flows
ISO/TS 26683-1	Intelligent transport systems – Freight land conveyance content identification and communication(FLC-CIC) – Part 1: Context, architecture and referenced standards
ITU-T L.1300	Best practices for green data centres – Study Group 5
ITU-T L.64	ID tag requirements for infrastructure and network elements management – Study Group 15
ITU-T M.3363	Requirements for data management in the telecommunication management network – StudyGroup 2
ITU-T SERIES D SUPP 4	Principles for increased adoption and use of mobile financial services (MFSs) through effectiveconsumer protection mechanisms – Study Group 3
ITU-T SERIES X SUPP 13	ITU-T X.1051 — Supplement on information security management users' guide for RecommendationITU-T X.1051 — Study Group 17
ITU-T SERIES X SUPP 32	ITU-T X.1058 — Supplement on codeof practice for personally identifiable information (PII) protectionfor telecommunications organizations — Study Group 17
ITU-T SERIES Y SUPP 40	Big data standardization roadmap – Study Group 13
ITU-T SERIES Y SUPP 55	ITU-T Y.3170-series – Machine learning in future networks including IMT-2020: Use cases – StudyGroup 13
ITU-T X.1058	Information technology — Security techniques — Code of practice for personally identifiableinformation protection — Study Group 17
ITU-T X.1147	Security requirements and framework for big data analytics in mobile Internet services — StudyGroup 17
ITU-T X.1250	Baseline capabilities for enhanced gbbal identity management and interoperability — Study Group 17
ITU-T X.1601	Security framework for cloud computing — Study Group 17
ITU-T X.1602	Security requirements for software as aservice application environments — Study Group 17
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing — Study Group 17
ITU-T X.1642	Guidelines for the operational security of cloud computing — Study Group 17
ITU-T Y.3174	Framework for data handling to enable machine learning in future networks including IMT-2020 –Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ITU-T Y.3604	Big data – Overview and requirements for data preservation – Study Group 13
ITU-T Y.4556	Requirements and functional architecture of smart residential community – Study Group 20

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
IEEE 1619-2018	IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices –

۵-۳-۳-۴- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۲: مدیریت هویت- اعتبارسنجی و احراز هویت (افراد، نهادها و دستگاه‌ها)

Issue 22 — Identity management – validation and authentication (People, Entity & Devices)	
ANSI INCITS 501	Information Technology – Security Features for SCSI Commands (SFSC)
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ANSI X9 TR-48	Card-Not-Present (CNP) Fraud Mitigation in the United States: Strategies for Preventing, Detecting,and Responding to a Growing Threat – ASCX9
ANSI X9.111	Penetration Testing within the Financial Services Industry – ASCX9
ANSI X9.73	Cryptographic Message Syntax – ASN.1 and XML – ASCX9
ANSI X9.84	Biometric Information Management and Security for theFinancial Services Industry
BSI PAS 11281	Connected automotive ecosystems – Impact of security on safety – Code of practice
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
BSI PAS 499	Code of practice for digital identification and strong customer authentication
BSI PAS 96	Guide to protecting and defending food and drink from deliberate attack
CEN 12830	Temperature recorders for the transport, storage and distribution of temperature sensitive goods –Tests, performance, suitability
CEN 16495	Air Traffic Management – Information security for organisations supporting civil aviation operations
CEN 419221-5	Protection Profiles for TSP Cryptographic Modules Part 5: Cryptographic Module for Trust Services
CEN EN 12896-5	Public transport – Reference data model – Part 5: Fare management
CEN/TS 16614-3	Public transport – Network and Timetable Exchange (NeTEx) Part 3: Public transport faresexchange format
DS DS/CWA 17302	City Resilience Development – Information Portal
DIN CEN/TS 16614-3	Public transport – Network and Timetable Exchange (NeTEx) – Part 3: Public transport fares exchangeformat; English version CEN/TS 16614-3:2016, only on CD-ROM
DIN SPEC 4997	Privacy by Blockchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN SPEC 91347	Integrated multi-functional Humble Lamppost (mHLa)

ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust ServiceProviders issuing certificates; Part 1: General requirements – V1.2.2
ETSI EN 319 521	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for ElectronicRegistered Delivery Service Providers – V1.1.1
ETSI EN 319 522-2	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2:Semantic contents — V1.1.1
ETSI EN 319 522-3	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3:Formats — V1.1.1; Includes Diskette
ETSI EN 319 522-4-3	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4:Bindings; Sub-part 3: Capability/requirements bindings – V1.1.1
ETSI EN 319 532-3 V1.2.1	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part3: Formats
ETSI GR PDL 001	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies – V1.1.1
ETSI GS ISI 002	Information Security Indicators (ISI); Event Model A security event classification model andtaxonomy — V1.2.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and RegulatoryConcerns — V1.1.1
ETSI GS NFV-SEC 014	Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANOComponents and Reference points – V3.1.1
ETSI SR 003 186	Electronic Signatures and Infrastructures (ESI) Testing interoperability and conformity activities to berun during the implementation and promotion of the framework ofdigital signatures — V2.1.1
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI SR 019 050	Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for ElectronicRegistered Delivery Services Applying Electronic Signatures – V1.1.1; Includes Diskette
ETSI TR 103 303	CYBER; Protection measures for ICT in the context of Critical Infrastructure – V1.1.1
ETSI TR 103 305-1	CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical SecurityControls — V3.1.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 604	User Group; User centric approach; Qualification of the interaction with the digital ecosystem – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TR 103 684	Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services – V1.1.1
ETSI TR 119 530	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Feasibility study: Interoperability profile between ETSI EN 319 532-based REM systems and PReM-basedsystems — V1.1.1
ETSI TS 133 501	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version

	16.4.0 Release 16)
ETSI TS 101 553-2	Core Network and Interoperability Testing (INT); Testing of the IBCF requirements; (3GPP Release 12);Part 2: Test Suite Structure and Test Purposes (TSS&TP) – V4.1.1
ETSI TS 102 412	Smart Cards; Smart Card Platform Requirements Stage 1 – V12.1.0; Release 12
ETSI TS 103 436	Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios – V1.2.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 645	CYBER; Cyber Security for Consumer Internet of Things – V1.1.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
ETSI TS 119 102-2	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES DigitalSignatures; Part 2: Signature Validation Report – V1.2.1; Includes Diskette
ETSI TS 119 403-3	Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers — V1.1.1
ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation – V1.1.1;Includes Diskette
ETSI TS 119 512	Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services — V1.1.1
ETSI TS 119 524-1	Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of ElectronicRegistered Delivery Services; Part 1: Testing conformance – V1.1.1
ETSI TS 119 534-1	Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability ofRegistered Electronic Mail Services; Part 1: Testing conformance – V1.1.1
ETSI TS 119 612	Electronic Signatures and Infrastructures (ESI); Trusted Lists – V2.2.1; Includes Diskette
ETSI TS 133 107	Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system(Phase 2+) (GSM); 3G security; Lawful interception architecture and functions – V15.6.0; 3GPP TS 33.107 version 15.6.0 Release 15
ETSI TS 133 180	LTE; Security of the mission critical service – V15.7.0; 3GPP TS 33.180 version 15.7.0 Release 15
ETSI TS 133 401	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture – V15.11.0; 3GPPTS 33.401 version 15.11.0 Release 15
IEC 60050-741	International Electrotechnical Vocabulary (IEV) – Part 741: Internet of Things (IoT) – Edition 1.0
IEC 60839-5-3	Alarm and electronic security systems – Part 5-3: Alarm transmission systems – Requirements forreceiving centre transceiver (RCT)

IEC 62443-2-4	Security for industrial automation and control systems – Part 2-4: Security program requirements forIACS service providers
IEC TR 62559-1	Use case methodology Part 1: Concept and processes in standardization
IEEE 1865	Maintenance and Test of Distributed Control Systems in Thermal Power Stations: GeneralRequirements and Definitions
IEEE 1865.2	Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal PowerStations: Operation Service and Management
IEEE 1934	Adoption of OpenFog Reference Architecture for Fog Computing
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 802.1CF	Recommended Practice for Network Reference Model and Functional Description of IEEE 802ضAccess Network – IEEE Computer Society
IEEE 802.1X	Local and Metropolitan Area Networks – Port-Based Network Access Control – IEEE ComputerSociety; Includes Access to Additional Content
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	PHD Cybersecurity Standards Roadmap – Version: 1.0
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 12812-1	Core banking – Mobile financial services Part 1: General framework
ISO 14721	Space data and information transfer systems – Open archival information system (OAIS) –Reference model
ISO 15118-1	Road vehicles – Vehicle togrid communication interface Part 1: General information and use-casedefinition
ISO 16484-5	Building automation and control systems (BACS) – Part 5: Data communication protocol(ISO 16484-5:2017)
ISO 20700	Guidelines for management consultancy services
ISO 22300	Security and resilience – Vocabulary (ISO 22300:2018)
ISO 9564-4	Financial services – Personal Identification Number (PIN) management and security – Part 4:Requirements for PIN handling in eCommerce for Payment Transactions
ISO TS 11633-1	Health informatics – Information security management for remote maintenance of medical devicesand medical information systems – Part 1: Requirements and risk analysis – First edition
ISO TS 12812-5	Core Banking – Mobile Financial Services – Part 5: Mobile Payments to Business – First Edition
ISO TS 23029	Web-service-based application programming interface (WAPI) in financial services – First edition
ISO/IEC 14776-454	Information technology – Small Computer System Interface (SCSI) – Part 454: SCSI PrimaryCommands — 4 (SPC-4)
ISO/IEC 14776-481	Information technology – Small computer system interface (SCSI) – Part 481: Part 481: SecurityFeatures for SCSI Commands (SFSC)
ISO/IEC 18013-1	Information technology – Personal identification – ISO-compliant driving licence – Part 1: Physicalcharacteristics and basic data set

ISO/IEC 18028-4	Information technology – Security techniques – IT network security – Part 4: Securing remote access
ISO/IEC 18370-2	Information technology – Security techniques – Blind digital signatures – Part 2: Discrete logarithmbased mechanisms
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and ofprotection of PII
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use — First Edition
ISO/IEC 20248	Information technology – Automatic identification and data capture techniques – Data structures –Digital signature meta structure – First Edition
ISO/IEC 20924	Internet of things (IoT) – Vocabulary
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation ofvirtualized servers
ISO/IEC 23006-3	Information technology – Multimedia service platform technologies – Part 3: Conformance andreference software — Third Edition
ISO/IEC 24759	Information technology – Security techniques – Test requirements for cryptographic modules –Third Edition
ISO/IEC 24760-1	IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management –Part 3: Practice
ISO/IEC 25023	Systems and software engineering – Systems and software Quality Requirements and Evaluation(SQuaRE) – Measurement of system and software product quality
ISO/IEC 27019	Information technology – Security techniques – Information security controls for the energyutility industry
ISO/IEC 27021	Information technology – Security techniques – Competence requirements for information securitymanagement systems professionals – First Edition
ISO/IEC 27036-4	Information technology – Security techniques – Information security for supplier relationships Part 4:Guidelines for security of cloud services
ISO/IEC 30107-1	Information technology – Biometric presentation attack detection Part 1: Framework
ISO/IEC 30118-2	Information technology – Open Connectivity Foundation (OCF) Specification – Part 2: Security specification
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derivedrequirements — First Edition
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC TR 29156	Information technology – Guidance for specifying performance requirements to meet security andusability needs in applications using biometrics
ISO/IEC TR 30125	Information technology – Biometrics used with mobile devices
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operationalenvironment
ISO/IEC TS 27008	Information technology – Security techniques – Guidelines for the assessment of informationsecurity controls

ISO/IEC/IEEE 8802-21	Information technology — Telecommunications and information exchange between systems —Local and metropolitan area networks — Specific requirements — Part 21: Media independent services framework
ISO/IEC/IEEE 8802-21-1	Information technology — Telecommunications and information exchange between systems — Localand metropolitan area networks — Part 21-1: Media independent services
ISO/TR 20526	Account-based ticketing state of the art report
ISO/TS 11633-1	Health informatics – Information security management for remote maintenance of medical devicesand medical information systems Part 1: Requirements and risk analysis
ISO/TS 12812-5	Core banking – Mobile financial services Part 5: Mobile payments to businesses
ISO/TS 23029	Web-service-based application programming interface (WAPI) in financial services
ITU-T G.7701	Common control aspects – Study Group 15
ITU-T H.550	Architecture and functional entities of vehicle gateway platforms – Study Group 16
ITU-T J.1	(Pre-Published) Terms, definitions and acronyms for television and sound transmission and integratedbroadband cable networks
ITU-T J.298	Requirements and technical specifications of a cable TV hybrid set-top box compatible with terrestrialand satellite TV transport — Study Group 9
ITU-T P.1502	Methodology for QoE testing of digital financial services — Study Group 12
ITU-T SERIES F SUPP 3	Overview of Telecom Finance (Finance 2.0) – Study Group 2
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T SERIES Y SUPP 53	ITU-T Y.4000-series – Internet of Things use cases – Study Group 20
ITU-T SERIES Y SUPP 56	ITU-T Y-series – Supplement on use cases of smart cities and communities – Study Group 20
ITU-T X.1038	Security requirements and reference architecture for software-defined networking — Study Group 17
ITU-T X.1039	Technical security measures forimplementation of ITU-T X.805 security dimensions — Study Group 17
ITU-T X.1087	Technical and operational countermeasures for telebiometric applications using mobile devices —Study Group 17
ITU-T X.1127	Functional security requirements and architecture for mobile phone anti-theft measures — StudyGroup 17
ITU-T X.1146	(Pre-Published) Secure protection guidelines for value-added services provided by telecommunication operators
ITU-T X.1258	Enhanced entity authentication based on aggregated attributes — Study Group 17
ITU-T X.1276	Authentication step-up protocol and metadata Version 1.0 — Study Group 17
ITU-T X.1277	Universal authentication framework — Study Group 17

ITU-T X.1331	Security guidelines for home area network (HAN) devices in smart grid systems — Study Group 17
ITU-T X.1450	Guidelines on hybrid authentication and key management mechanisms in the client-server model —Study Group 17
ITU-T X.1605	Security requirements of public Infrastructure as aService (IaaS) in cloud computing — Study Group 17
ITU-T X.1631	Information technology — Security techniques — Code of practice for information security controlsbased on ISO/IEC 27002 for cloud services — Study Group 17
ITU-T X.1642	Guidelines for the operational security of cloud computing — Study Group 17
ITU-T Y.2342	Scenarios and capability requirements of blockchain in next generation network evolution – StudyGroup 13
ITU-T Y.4459	Digital entity architecture framework for Internet of things interoperability – Study Group 20
SAE J3101	Hardware Protected Security for Ground Vehicles
SAE PT-179	Commercial Aviation Cyber Security: Current State and Essential Reading – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SNZ AS/NZS 62676.1.1	Video surveillance systems for use in security applications Part 1.1: System requirements – General
UL 827 BULLETIN	UL Standard for Safety Central-Station Alarm Services – COMMENTS DUE: June 22, 2020

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO 17442:2019	Financial services – Legal entity identifier (LEI)
ISO/CD 24366	Natural Persons Identifier
CAN/CIOSC 103-1	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
Pan-Canadian Trust Framework	A collaborative approach to developing a Pan-Canadian Trust Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 103-3	Digital trust and identity – Part 3: Digital credentials
CAN/CIOSC 103-4	Digital trust and identity – Part 4: Digital wallets
IEEE P1363.3/D9	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings
IEEE 802.1AR-2018	IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity
IEEE 2410-2019	IEEE Standard for Biometric Open Protocol
DIACC PCTF 01	Pan-Canadian Trust Framework (PCTF) Model v1.0
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent: Component Overview and ConformanceProfile v1.0
DIACC PCTF 03	Pan-Canadian Trust Framework (PCTF) Authentication: Component Overview and

	ConformanceProfile v1.0
DIACC PCTF 04	Pan-Canadian Trust Framework (PCTF) Privacy: Component Overview and Conformance Profile v1.0
DIACC PCTF 05	Pan-Canadian Trust Framework (PCTF) Verified Person: Component Overview and ConformanceProfile v1.0
DIACC PCTF 06	Pan-Canadian Trust Framework (PCTF) Verified Organization: Component Overview andConformance Profile v1.0
DIACC PCTF 07	Pan-Canadian Trust Framework (PCTF) Credentials (Relationship & Attributes): Component Overviewand Conformance Profile v1.0
DIACC PCTF 08	Pan-Canadian Trust Framework (PCTF) Infrastructure (Technology & Operations): ComponentOverview and Conformance Profile v1.0
DIACC PCTF 09	Pan-Canadian Trust Framework (PCTF) Assessment v1.0
DIACC PCTF 10	Pan-Canadian Trust Framework (PCTF) Glossary V1.0

۵-۳-۳-۵- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۳: به اشتراک‌گذاری، تبادل و یکپارچه‌سازی داده‌ها

Issue 23 — Data Sharing, Exchanging, and Integration	
ISO/IEC TR 29144	Information technology – Biometrics – The use of biometric technology in commercial IdentityManagement applications and processes
CEN EN 16570	Information technology – Notification of RFID – The information sign and additional information to beprovided by operators of RFID application systems
ISO 20614	Information and documentation – Data exchange protocol for interoperability and preservation
DIN 66398	Guideline for development of a concept for data deletion with derivation of deletion periods forpersonal identifiable information
ANSI INCITS 459	Information Technology – Requirements for the Implementation and Interoperability of Role BasedAccess Control
ANSI INCITS 398	Information Technology Common Biometric Exchange Formats Framework (CBEFF)
ASTM E2468	Standard Practice for Metadata to Support Archived Data Management Systems
ISO/IEC 24713-3	Information technology – Biometric profiles for interoperability and data exchange Part 3: Biometrics-based verification and identification of seafarers
NFPA 951	Guide to Building and Utilizing Digital Information – Effective date: 4/12/2015
ISO/IEC 18598	Information technology – Automated infrastructure management (AIM) systems – Requirements,data exchange and applications
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy informationmanagement – Requirements and guidelines
ISO/IEC TS 27008	Information technology – Security techniques – Guidelines for the assessment of informationsecurity controls

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 100-9	Data Governance – Part 9: Zero Copy Integration
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 106-1	Discovery and management of Digital Twins for built environments – Part 1: Discovery
CAN/CIOSC 106-2	Discovery and management of Digital Twins for built environments – Part 2: Management
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
IEEE/IEC 61671-2-2016	IEC/IEEE International Standard for Automatic Test Markup Language (ATML) Instrument Description
IEEE 1671.2	IEEE Trial-Use Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic TestEquipment and Test Information via XML: Exchanging Instrument Descriptions
IEEE 1671.3	IEEE Standard forAutomatic Test Markup Language (ATML) for Exchanging Automatic TestInformation via XML (eXtensible Markup Language): Exchanging UUT (Unit Under Test) DescriptionInformation
IEEE 1671.4	IEEE Standard forAutomatic Test Markup Language (ATML) for Exchanging Automatic TestInformation via eXtensible Markup Language (XML): Exchanging Test Configuration Information
IEEE 1671.5	IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic TestInformation via XML:Exchanging Test Adapter Information
IEEE 1671.6	IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic TestInformation via XML: Exchanging Test Station Information
ISO/IEC/IEEE 18881:2016	ISO/IEC/IEEE Information technology- Ubiquitous green community control network protocol
IEEE P802.11bb	IEEE Standard for Information technology – Telecommunications and information exchange betweensystems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LANMedium Access Control (MAC) and Physical Layer (PHY) Specifications
CSA Z8003	Health care design research and evaluation

۵-۳-۳-۶- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۴: واسطه‌های قابل اعتماد داده‌ها

Issue 24 — Trusted Data Intermediaries	
ETSI TS 133 501	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.4.0 Release 16)
ISO TR 20526	Account-based ticketing state of the art report – First Edition
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
ISO/IEC 15944-12	Information technology — Business operational view Part 12: Privacy protection requirements (PPR) oninformation life cycle management (ILCM) and EDI of personal information (PI)
ISO/IEC 17788	Information technology – Cloud computing – Overview and vocabulary
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture (ISO/IEC 17789:2014)
ISO/IEC 17826	Information technology – Cloud Data Management Interface (CDMI)
ISO/IEC 19086-1	Information technology – Cloud computing – Service level agreement (SLA) framework – Part 1:Overview and concepts (ISO/IEC 19086-1:2016)
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and ofprotection of PII
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability – First Edition
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation ofvirtualized servers
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management –Part 3: Practice
ISO/IEC 27000	Information technology – Security techniques – Information security management systems –Overview and vocabulary
ISO/IEC 27009	Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 –Requirements (ISO/IEC 27009:2016)
ISO/IEC 27018	Information technology – Security techniques – Code of practice for protection of personallyidentifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27036-4	Information technology – Security techniques – Information security for supplier relationships – Part4: Guidelines for security of cloud services
ISO/IEC 27701	Expert commentary BS ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 andISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC 30141	Internet of Things (IoT) – Reference architecture
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC38500 to the governance of data – First Edition
ISO/IEC TR 20000-9	Information technology – Service management Part 9: Guidance on the application of ISO/IEC20000-1 to cloud services
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derivedrequirements — First Edition
ISO/IEC TR 22678	Information technology – Cloud computing – Guidance for policy development
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of

	multi-sourced data
ISO/IEC TR 23187	Information technology – Cloud computing – Interacting with cloud service partners (CSNs) –First edition
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape – First edition
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing – First Edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO/IEC TS 23167	Information technology – Cloud computing – Common technologies and techniques – First edition
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
n/a	Exploring Data Trust Certifications
CAN/CIOSC 103-1	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
Pan-Canadian Trust Framework	A collaborative approach to developing a Pan-Canadian Trust Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship

۵-۳-۳-۷- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۵: مجوز به اشتراک‌گذاری و جمع‌آوری (گردآوری) داده‌ها

Issue 25 —Authorization for data collection and sharing	
ANSI INCITS 172	Information Technology – American National Standard Dictionary of Information Technology (ANSDIT)
ASHRAE 135	BACnet – A Data Communication Protocol for Building Automation and Control Networks
ASHRAE 201	Facility Smart Grid Information Model
ASTM E1578	Standard Guide for Laboratory Informatics
AWWA G410	Business Practices for Operation and Management
BSI BS 10012	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations

BSI PAS 1085	Manufacturing – Establishing and implementing a security-minded approach – Specification
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
BSI PAS 180	Smart cities – Vocabulary
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and informationservices
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach –CORR: May 30, 2018
CEN EN 14484	Health informatics – International transfer of personal health data covered by the EU data protectiondirective — High level security policy
CEN EN 14485	Health informatics – Guidance for handling personal health data in international applications in thecontext of the EU data protection directive; German version EN 14485:2003, text in English
CEN/TS 17470	Service model for social carealarms
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
DS DS/CWA 17145-1	Ethics assessment for research and innovation – Part 1: Ethics committee
ETSI GS INS 009	Identity and access management for Networks and Services (INS); Security and privacy requirementsfor collaborative cross domain network monitoring – V1.1.1
ETSI GS MOI 002	Measurement Ontology for IP traffic (MOI); Requirements for IP traffic measurement ontologiesdevelopment — V1.1.1
ETSI SR 002 564	Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth – V2.0.0
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI TR 102 202	Human Factors (HF); Human Factors of work in call centres – V1.1.2
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 305	CYBER; Critical Security Controls for Effective Cyber Defence – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
ETSI TS 129 240	Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Generic User Profile (GUP); Stage 3;Network – V15.0.0; 3GPP TS 29.240 version 15.0.0 Release 15
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 26514	Adoption of ISO/IEC 26514:2008 Systems and Software Engineering – Requirements for Designersand Developers of User Documentation – IEEE Computer Society
IEEE WHITE PAPER 3DBP IC	IEEE 3D BODY PROCESSING INDUSTRY CONNECTIONS (3DBP IC): COMMUNICATION, SECURITY,AND PRIVACY
IEEE WHITE	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with

PAPER-0	Blockchain
ISO 13606-4	Health informatics – Electronic health record communication – Part 4: Security
ISO 18308	Health informatics – Requirements for an electronic health record architecture
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO 19650-5	Organization and digitization of information about buildings and civil engineering works, includingbuilding information modelling (BIM) – Information management using building information modelling – Part 5: Security-minded approach to information management – First edition
ISO 20252	Market, opinion and social research, including insights and data analytics – Vocabulary and servicerequirements
ISO 22857	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal healthdata — Second Edition
ISO 24100	Intelligent transport systems – Basic principles for personal data protection in probe vehicleinformation services
ISO 24978	Intelligent transport systems – ITS Safety and emergency messages using any available wirelessmedia – Data registry procedures (ISO 24978:2009); English version EN ISO 24978:2009
ISO 25237	Health informatics – Pseudonymization (ISO 25237:2017)
ISO 26000	Guidance on social responsibility (ISO 26000:2010)
ISO 29134	Information technology – Security techniques – Guidelines for privacy impact assessment(ISO/IEC 29134:2017)
ISO 35001	Biorisk management for laboratories and other related organisations – First edition
ISO 37156	Smart community infrastructures – Guidelines on data exchange and sharing for smart community infrastructures
ISO TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap – Part 2: Architecturalcomponents and maturity model – First Edition
ISO TR 17427-3	Intelligent transport systems – Cooperative ITS – Part 3: Concept of operations (ConOps) for 'core'systems — First Edition
ISO TR 17427-7	Intelligent transport systems – Cooperative ITS – Part 7: Privacy aspects – First Edition
ISO TR 22221	Health informatics Good principles and practices for a clinical data warehouse – First Edition
ISO TR 22758	Biotechnology – Biobanking – Implementation guide for ISO 20387 – First edition
ISO TS 12812-5	Core Banking – Mobile Financial Services – Part 5: Mobile Payments to Business – First Edition
ISO TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment — First Edition
ISO TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information — First Edition
ISO TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care – First Edition
ISO TS 21089	Health informatics – Trusted end-toend information flows – First Edition
ISO TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles –First Edition
ISO TS 22220	Health informatics – Identification of subjects of health care – Second Edition
ISO TS 29585	Health informatics – Deployment of a clinical data warehouse – First Edition
ISO TS 37107	Sustainable cities and communities – Maturity model for smart sustainable communities – First edition

ISO/IEC 15504-6	Information technology – Process assessment – Part 6: An exemplar system life cycle processassessment model — First Edition
ISO/IEC 15944-9	Information technology – Business Operational View – Part 9: Business transaction traceabilityframework for commitment exchange
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ISO/IEC 18028-1	Information technology – Security techniques – IT network security Part 1: Network security management
ISO/IEC 18384-2	Information technology – Reference Architecture for Service Oriented Architecture (SOA RA) Part 2:Reference Architecture for SOA Solutions
ISO/IEC 19790	Information technology – Security techniques – Security requirements for cryptographic modules –Second Edition; Corrected version 12/15/2015
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability – First Edition
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use
ISO/IEC 20748.1	Information technology for learning, education and training – Learning analytics interoperability Part 1:Reference model
ISO/IEC 20748.2	Information technology for learning, education and training – Learning analytics interoperability Part 2:System requirements
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC 20944-1	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) Part 1:Framework, common vocabulary, and common provisions for conformance
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 23092-1	Information technology – Genomic information representation – Part 1: Transport and storage ofgenomic information
ISO/IEC 23092-2	Information technology – Genomic information representation – Part 2: Coding of genomicinformation — First edition
ISO/IEC 23092-3	Information technology – Genomic information representation – Part 3: Metadata and applicationprogramming interfaces (APIs) – First edition
ISO/IEC 24760-1	Information technology – Security techniques – A framework for identity management – Part 1:Terminology and concepts
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2:Reference architecture and requirements – First Edition
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management – Part 3: Practice
ISO/IEC 27033-1	Information technology – Security techniques – Network security – Part 1: Overview and concepts
ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy informationmanagement – Requirements and guidelines
ISO/IEC 29155-4	Systems and software engineering – Information technology project performance benchmarkingframework Part 4: Guidance for data collection and maintenance
ISO/IEC 30141	Internet of Things (loT) – Reference Architecture
ISO/IEC/IEEE 12207	Systems and software engineering – Software life cycle processes
ISO/IEC/IEEE 15288	Systems and software engineering – System life cycle processes – First Edition

ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems,software, and services information
ISO/IEC/IEEE 24748-1	Systems and software engineering – Life cycle management Part 1: Guidelines for life cycle management
ISO/IEC/IEEE 29148	Systems and software engineering – Life cycle processes – Requirements engineering
ISO/IEC/TR 13335-4	Information Technology – Guidelines for the Management of IT Security – Part 4: Selection ofSafeguards (TECHNICAL REPORT)
ISO/IEC/TR 20748-1	Information technology for learning, education and training – Learning analytics interoperability Part 1:Reference model
ISO/IEC/TR 20748-2	Information technology for learning, education and training – Learning analytics interoperability Part 2:System requirements – CORR: August 31, 2018
ISO/IEC/TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC/TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC/TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commericalapplications Part 1: General guidance
ISO/IEC/TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC/TR 29144	Information technology – Biometrics – The use of biometric technology in commercial IdentityManagement applications and processes
ISO/IEC/TR 29196	Guidance for biometric enrolment
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap Part 2: Architectural componentsand maturity model
ISO/TR 17424	Intelligent transport systems – Cooperative systems – State of the art of Local Dynamic Mapsconcepts — CORR: June 30, 2015
ISO/TR 17427-3	Intelligent transport systems – Cooperative ITS Part 3: Concept of operations (ConOps) for‘core’ systems
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/TR 17427-9	Intelligent transport systems – Cooperative ITS Part 9: Compliance and enforcement aspects
ISO/TR 17465-2	Intelligent transport systems – Cooperative ITS – Part 2: Guidelines for standards documents
ISO/TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment – CORR: February 28, 2014
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information
ISO/TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care(ISO/TS 19256:2016); English version CEN ISO/TS 19256:2017
ISO/TS 21089	Health informatics – Trusted end-to-end information flows
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse

ISO/TS 37107	Sustainable cities and communities – Maturity model for smart sustainable communities
ITU-T M.3363	Requirements for data management in the telecommunication management network – Study Group 2
ITU-T SERIES X SUPP 32	ITU-T X.1058 — Supplement on codeof practice for personally identifiable information (PII) protectionfor telecommunications organizations — Study Group 17
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T SERIES Y SUPP 56	ITU-T Y-series – Supplement on use cases of smart cities and communities – Study Group 20
ITU-T X.1045	Security service chain architecture for networks and applications — Study Group 17
ITU-T X.1209	Capabilities and their context scenarios for cybersecurity information sharing and exchange —Study Group 17
ITU-T X.1361	Security framework for the Internet of things based on the gateway model — Study Group 17
ITU-T X.1363	(Pre-Published) Technical framework of personally identifiable information (PII) handling in Internet ofthings (IoT) environment
ITU-T Y.2705	Minimum security requirements for the interconnection of the Emergency TelecommunicationsService (ETS) — Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.4117	Requirements and capabilities of the Internet of things for support of wearable devices and relatedservices — Study Group 20
ITU-T Y.4500.2	oneM2M – Requirements – Study Group 20
ITU-T Y.4555	Service functionalities of self-quantification over Internet of things – Study Group 20
ITU-T Y.4904	Smart sustainable cities maturity model – Study Group 20
SAE AIR6904	Rationale, Considerations, and Framework for Data Interoperability for Health Management within theAerospace Ecosystem
SAE EIA-836B	Configuration Management Data Exchange and Interoperability – Formerly TechAmerica EIA-836B;Includes Access to Additional Content
SNZ HB 246	Guidelines for managing risk in sport andrecreation organizations
UL 2800 BULLETIN	UL Standard for Safety Medical Device Interoperability – COMMENTS DUE: November 5, 2018
ULC CAN/ULC-S576	STANDARD FOR MASS NOTIFICATION SYSTEM EQUIPMENT AND ACCESSORIES – SECOND EDITION
ISO TR 14872	Health informatics – Identification of medicinal products – Core principles for maintenance ofidentifiers and terms — First edition
ISO 18750	Intelligent transport systems – Co-operative ITS – Local dynamic map – First Edition
ISO/IEC TR 20748-1	Information technology for learning, education and training – Learning analytics interoperability –Part 1: Reference model — First Edition
ETSI TS 102 573	Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signingand/or storing data objects — V2.1.1
AWWA G430	Security Practices for Operation and Management
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
IEEE P3333.2.3	Standard for Three-Dimensional (3D) Medical Data Management

۵-۳-۳-۸- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۶: رمزنگاری

Issue 26- Encryption	
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ANSI INCITS 504-3	Information Technology – Generic Identity Command – Part 3: GICS Platform Testing Requirements
ANSI X9 TR-48	Card-Not-Present (CNP) Fraud Mitigation in the United States: Strategies for Preventing, Detecting,and Responding to a Growing Threat – ASCX9
ANSI X9.69	Framework for Key Management Extensions
ANSI X9.73	Cryptographic Message Syntax – ASN.1 and XML – ASCX9
ASHRAE 135	BACnet – A Data Communication Protocol for Building Automation and Control Networks
ASHRAE HVAC APPLICATIONS SI CH 40	COMPUTER APPLICATIONS
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code ofpractice for implementation of BS 10008-1
BSI DD ENV 13608-1	Health Informatics – Security for Healthcare Communication – Part 1: Concepts and Terminology
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
BSI PD CEN/TR 16742	Intelligent transport systems – Privacy aspects inITS standards and systems inEurope
CEN 15320	Identification card systems – Surface transport applications – Interoperable Public TransportApplications — Framework
CEN 15531-2	Public transport – Service interface for real-time information relating to public transport operations –Part 2: Communications; English version EN 15531-2:2015
CEN 16312	Intelligent transport systems – Automatic Vehicle and Equipment Registration (AVI/AEI) – Interoperableapplication profile forAVI/AEI and Electronic Register Identification using dedicated shortrange communication; English version EN 16312:2013

CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
DIN 66398	Guideline for development of a concept for data deletion with derivation of deletion periods forpersonal identifiable information
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN CEN/TS 16634	Personal identification – Recommendations for using biometrics in European Automated BorderControl; English version CEN/TS 16634:2014
ETSI GR NFV 001	Network Functions Virtualisation (NFV); Use Cases – V1.2.1
ETSI GR NFV-SEC 003	Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance – V1.2.1
ETSI GR NFV-SEC 009	Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approachesfor multi-layer host administration — V1.2.1
ETSI GR QSC 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework – V1.1.1
ETSI GR QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios – V1.1.1
ETSI GR QSC 004	Quantum-Safe Cryptography; Quantum-Safe threat assessment – V1.1.1
ETSI GR QSC 006	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric keysizes — V1.1.1
ETSI GS ENI 005	Experiential Networked Intelligence (ENI); System Architecture – V1.1.1
ETSI GS INS 005	Identity and access management for Networks and Services; Requirements of an EnforcementFramework in a Distributed Environment – V1.1.1
ETSI GS NFV-SEC 001	Network Functions Virtualisation (NFV); NFV Security; Problem Statement – V1.1.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and RegulatoryConcerns — V1.1.1
ETSI GS NFV-SEC 013	Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoringspecification — V3.1.1
ETSI GS NGP 001	Next Generation Protocols (NGP); Scenario Definitions – V1.3.1
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI TR 102 935	Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart GridNetworks; Impact of Smart Grids on M2M platform – V2.1.1
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 305	CYBER; Critical Security Controls for Effective Cyber Defence – V1.1.1
ETSI TR 103 305-1	CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls – V3.1.1
ETSI TR 103 305-3	CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations — V2.1.1

ETSI TR 103 308	CYBER; Security baseline regarding LI and RD for NFV and related platforms – V1.1.1
ETSI TR 103 376	SmartM2M; IoT LSP use cases and standards gaps – V1.1.1
ETSI TR 103 456	CYBER; Implementation of the Network and Information Security (NIS) Directive – V1.1.1
ETSI TR 103 509	SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well – V1.1.1
ETSI TR 103 533	SmartM2M; Security; Standards Landscape and best practices – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 102 412	Smart Cards; Smart Card Platform Requirements Stage 1 – V12.1.0; Release 12
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI GS MOI 002	Measurement Ontology for IP traffic (MOI); Requirements for IP traffic measurement ontologiesdevelopment — V1.1.1
ETSI TR 102 935	Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart GridNetworks; Impact of Smart Grids on M2M platform – V2.1.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
ETSI TR 103 582	EMTEL; Study of use cases and communications involving IoT devices in provision of emergencysituations — V1.1.1
ETSI TS 103 485	CYBER; Mechanisms for privacy assurance and verification – V1.1.1
ETSI TR 102 937	eCall communications equipment; Conformance to EU vehicle regulations, R&TTE, EMC & LVDirectives, and EU regulations for eCall implementation – V1.1.1
IEC 62443-2-4	Security for industrial automation and control systems – Part 2-4: Security program requirements forIACS service providers
IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System securityrequirements and security levels
IEC 62443-4-2	Security for industrial automation and control systems Part 4-2: Technical security requirements forIACS components
IEC/TR 62939-1	Smart grid user interface — Part 1: Interface overview and country perspectives — Edition 1.0
IEC/TS 62045-1	Multimedia security – Guideline for privacy protection of equipment and systems in and out of use –Part 1: General
IEEE 1619	Cryptographic Protection of Data on Block- Oriented Storage Devices – IEEE Computer Society
IEEE 1619.2	Wide-Block Encryption for Shared Storage Media – IEEE Computer Society

IEEE 1703	Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complementthe Utility Industry End Device Data Tables
IEEE 23026	Systems and software engineering – Engineering and management of websites for systems,software, and services information
IEEE 2410	Biometric Open Protocol
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	PHD Cybersecurity Standards Roadmap – Version: 1.0
IEEE 2600	Information Technology: Hardcopy Device and System Security – IEEE Computer Society
ISO 11073-90101	Health informatics – Point-of-care medical device communication – Part 90101: Analyticalinstruments — Point-of-care test
ISO 16484-3	Building automation and control systems (BACS) – Part 3: Functions
ISO 16484-5	Building automation and control systems (BACS) Part 5: Data communication protocol — AMD: May 31,2020
ISO 20214	Space data and information transfer systems – Security architecture for space data systems
ISO TR 11636	Health Informatics – Dynamic on-demand virtual private network for health informationinfrastructure — First Edition
ISO TR 17427-3	Intelligent transport systems – Cooperative ITS – Part 3: Concept of operations (ConOps) for 'core'systems — First Edition
ISO TR 23244	Blockchain and distributed ledger technologies – Privacy and personally identifiable informationprotection considerations – First edition
ISO TR 23455	Blockchain and distributed ledger technologies – Overview of and interactions between smartcontracts in blockchain and distributed ledger technology systems – First edition
ISO TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment — First Edition
ISO TS 21089	Health informatics – Trusted end-toend information flows – First Edition
ISO TS 22220	Health informatics – Identification of subjects of health care – Second Edition
ISO TS 29585	Health informatics – Deployment of a clinical data warehouse – First Edition
ISO/IEC 15408-2	Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Securityfunctional components (ISO/IEC 15408-2:2008)
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ISO/IEC 18033-6	IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC 25023	Systems and software engineering – Systems and software Quality Requirements and Evaluation(SQuaRE) – Measurement of system and software product quality

ISO/IEC 27017	Information technology – Security techniques – Code of practice for information security controlsbased on ISO/IEC 27002 for cloud services
ISO/IEC 27033-1	Information technology – Security techniques – Network security – Part 1: Overview and concepts
ISO/IEC 27033-3	Information technology – Security techniques – Network security Part 3: Reference networkingscenarios – Threats, design techniques and control issues
ISO/IEC 27040	Information technology – Security techniques – Storage security – CORR: September 30, 2016
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiableinformation protection – First Edition
ISO/IEC 30118-2	Information technology – Open Connectivity Foundation (OCF) Specification Part 2: Security specification
ISO/IEC 30136	Information technology – Performance testing of biometric template protection schemes
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TR 22678	Information technology – Cloud computing – Guidance for policy development
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence –First edition
ISO/IEC TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commericalapplications Part 1: General guidance
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 29181-2	Information technology – Future Network – Problem statement and requirements Part 2: Namingand addressing
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing
ISO/IEC TR 30166	Internet of Things (IoT) – Industrial IoT
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in theiroperational environment
ISO/IEC TS 23167	Information technology – Cloud computing – Common technologies and techniques
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems,software, and services information
ISO/TR 11636	Health Informatics – Dynamic on-demand virtual private network for health information infrastructure

ISO/TR 17427-3	Intelligent transport systems – Cooperative ITS Part 3: Concept of operations (ConOps) for‘core’ systems
ISO/TR 18307	Health informatics interoperability and compatibility in messaging and communication standardsKey characteristics
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment
ISO/TS 21089	Health informatics – Trusted end-to-end information flows
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles
ISO/TS 22220	Health informatics – Identification of subjects of health care
ISO/TS 27790	Health informatics – Document registry framework
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO 25237	Health informatics – Pseudonymization
ISO/IEC TS 27008 – TC	TC – Tracked Changes (Redline) – Information technology – Security techniques – Guidelines for the assessment of information security controls – Compares PD ISO/IEC TS 27008:2019 with PD ISO/IECTR 27008:2011
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use — First Edition
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO/TS 14265	Health Informatics – Classification of purposes for processing personal health information
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosureof personal health information
ISO 22857	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal healthdata — Second Edition
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO/IEC TS 20748-4:20	Information technology for learning, education and training – Learning analytics interoperability – Part4: Privacy and data protection policies
ISO/IEC 27011	Information technology – Security techniques – Code of practice for Information security controlsbased on ISO/IEC 27002 for telecommunications organizations
ISO/IEC 29100	Information technology — Security techniques — Privacy framework (ISO/IEC 29100:2011, includingAmd 1:2018)
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment
ISO 5127	Information and documentation Vocabulary

ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/IEC 19506	Information technology – Object Management Group Architecture-Driven Modernization (ADM) –Knowledge Discovery Meta-Model (KDM)
ISO/IEC 27034-1	Information technology – Security techniques – Application security Part 1: Overview and concepts –CORR: February 28, 2014
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiableinformation protection
ITU-T H.810	(Pre-Published) Interoperability design guidelines for personal connected health systems: Introduction
ITU-T J.191	IP feature package to enhance cable modems
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T X.1039	Technical security measures forimplementation of ITU-T X.805 security dimensions — Study Group 17
ITU-T X.1045	Security service chain architecture for networks and applications — Study Group 17
ITU-T X.1361	Security framework for the Internet of things based on the gateway model — Study Group 17
ITU-T X.1401	Security threats to distributed ledger technology — Study Group 17
ITU-T X.1602	Security requirements for software as aservice application environments — Study Group 17
ITU-T X.1642	Guidelines for the operational security of cloud computing — Study Group 17
ITU-T X.894	(Pre-Published) Generic applications of ASN.1 Cryptographic Message Syntax
ITU-T Y.2342	Scenarios and capability requirements of blockchain in next generation network evolution –Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ITU-T Y.3505	Cloud computing – Overview and functional requirements for data storage federation –Study Group 13
ITU-T Y.3509	Cloud computing – Functional architecture for data storage federation – Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3524	Cloud computing maturity requirements and framework – Study Group 13
ITU-T Y.3800	Overview on networks supporting quantum key distribution Corrigendum 1 – Study Group 13
ITU-T Y.4459	Digital entity architecture framework for Internet of things interoperability – Study Group 20

ITU-T Y.3501	Cloud computing – Framework and high-level requirements – Study Group 13
ITU-T H.780	Digital signage: Service requirements and IPTV-based architecture – Study Group 16
NEMA C12.22	Protocol Specification for Interfacing to Data Communication Networks
UL CAN/UL 2900-1	UL Standard for Safety Software Cybersecurity for Network-Connectable Products, Part 1: GeneralRequirements – First Edition; Reprint with Revisions Through and Including June 5, 2020
UL SUBJECT 2900-1	UL Outline for Investigation Software Cybersecurity for Network- Connectable Products, Part 1:General Requirements — Issue 2

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
IEEE Std 2410-2019	IEEE Standard for Biometric Open Protocol
IEEE Std 1363.3-2013	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings
IEEE 1619.1-2018	IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices
IEEE 1735-2014	IEEE Recommended Practice for Encryption and Management of Electronic Design IntellectualProperty (IP)
IEEE P802.15.4y	IEEE Draft Standard for Low-Rate Wireless Networks Amendment Defining Support for AdvancedEncryption Standard (AES)-256 Encryption and Security Extensions
IEEE 802.1AEcg-2017	IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Security –Amendment 3: Ethernet Data Encryption devices
IEEE/ISO/IEC 8802-1AE:2013/Amd.3-2018 -	IEEE/ISO/IEC International Standard — Information technology — Telecommunications and informationexchange between systems — Local and metropolitan area networks — Part 1AE: Media access control(MAC) security AMENDMENT 3: Ethernet data encryption devices
IEEE 1609.2b-2019	IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications andManagement Messages – Amendment 2 – PDU Functional Types and Encryption Key Management

IEEE 8802-1AE:2013/ Amd.1-2015	ISO/IEC/IEEE International Standard for Information technology — Telecommunications and information exchan+F43ge between systems — Local and metropolitan area networks — Part 1AE: Media access control (MAC) security — AMENDMENT 1: Galois Counter Model — Advanced EncryptionStandard-256 (GCMAES-256) Cipher Suite
IEEE ST 429-6:2006 Am1:2018	SMPTE Amendment – D-Cinema Packaging – MXF Track File Essence Encryption

۵-۳-۳-۹- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۷: مدیریت هستی‌شناسی (فهرستی از مفاهیم و دسته‌بندی‌های داده و ارتباط بین آن‌ها)

Issue 27 — Management of ontologies	
ITU-T Y.2076	Semantics based requirements and framework of the Internet of things – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ITU-T Y.4203	Requirements of things description in the Internet of things – Study Group 20
ITU-T Y.4461	Framework of open data in smart cities – Study Group 20
ISO/TS 13606-4	Health informatics – Electronic health record communication – Part 4: Security
ETSI TR 103 537	SmartM2M; Plugtests™ preparation on Semantic Interoperability – V1.1.1
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
ETSI GS MOI 010	Measurement Ontology for IP traffic (MOI); Report on information models for IP traffic measurement – V1.1.1
ANSI INCITS 532	Information Technology – Vocabulary Description and Management
DIN SPEC 91349	Taxonomy of Rules and Regulations in Smart Data; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A ConcreteApproach — V1.1.1
ETSI TR 103 411	SmartM2M; Smart Appliances; SAREF extension investigation – V1.1.1
ETSI TR 103 509	SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well – V1.1.1
ISO 13606-1	Health informatics – Electronic health record communication – Part 1: Reference model (ISO 13606-1:2019); English version EN ISO 13606-1:2019
ISO 8000-115	Data quality – Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolutionrequirements — First Edition
ISO 8000-116	Data quality Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 toauthoritative legal entity identifiers
ISO 8000-120	Data quality – Part 120: Master data: Exchange of characteristic data: Provenance – First Edition
ISO 8000-130	Data quality – Part 130: Master data: Exchange of characteristic data: Accuracy – First Edition
ISO 8000-140	Data quality – Part 140: Master data: Exchange of characteristic data: Completeness – First Edition
ISO 8000-2	Data quality Part 2: Vocabulary

ISO/IEC 11179-1	Information technology – Specification and standardization of data elements – Part 1: Framework forthe specification and standardization of data elements
ISO/IEC 11179-3	Information technology – Metadata registries (MDR) – Part 3: Registry metamodel and basic attributes
ISO/IEC 11179-5	Information technology – Metadata registries (MDR) – Part 5: Naming and Identification principles
ISO/IEC 11179-6	Information technology – Metadata registries (MDR) Part 6: Registration
ISO/IEC 11179-7	Information technology – Metadata registries (MDR) – Part 7: Metamodel for data set registration
ISO/IEC 15026.1	Systems and software engineering – Systems and software assurance Part 1: Conceptsand vocabulary
ISO/IEC 16680	Information technology – The Open Group Service Integration Maturity Model (OSIMM)
ISO/IEC 19763-1	Information technology – Metamodel framework for interoperability (MFI) – Part 1: Reference model
ISO/IEC 19763-3	Information technology – Metamodel framework for interoperability (MFI) – Part 3: Metamodel forontology registration
ISO/IEC 19763-5	Information technology – Metamodel framework for interoperability (MFI) – Part 5: Metamodel forprocess model registration
ISO/IEC 19763-6	Information technology – Metamodel framework for interoperability (MFI) – Part 6: RegistrySummary — First Edition
ISO/IEC 19763-7	Information technology – Metamodel framework for interoperability (MFI) – Part 7: Metamodel forservice model registration
ISO/IEC 20547-3	Information technology – Big data reference architecture Part 3: Reference architecture
ISO/IEC 24707	Information technology – Common Logic (CL): a framework for a family of logic-based languages
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability
ISO/IEC TR 19583-1	Information technology – Concepts and usage of metadata Part 1: Metadata concepts
ISO/IEC TR 20547-5	Information technology – Big data reference architecture – Part 5: Standards roadmap
ISO/IEC TR 20943-1	Information technology Procedures for achieving metadata registry (MDR) content consistency Part 1:Data elements
ISO/IEC TR 20943-5	Information technology – Procedures for achieving metadata registry content consistency – Part 5:Metadata mapping procedure – First Edition
ISO/IEC TR 20943-6	Information technology – Procedures for achieving metadata registry content consistency – Part 6:Framework for generating ontologies – First Edition
ISO/IEC TS 19763-13	Information technology – Metamodel framework for interoperability (MFI) Part 13: Metamodel for formdesign registration

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
IEEE Std 2755-2017	IEEE Guide for Terms and Concepts in Intelligent Process Automation
IEEE Std 1636.1-2018	IEEE Standard for Software Interface for Maintenance Information Collection and Analysis (SIMICA):Exchanging Test Results and Session Information via the eXtensible Markup Language (XML)
IEEE 11073-10101-2019	ISO/IEEE International Standard — Health informatics — Point-of-care medical device communication —Part 10101: Nomenclature AMENDMENT 1: Additional definitions
ISO/IEC/IEEE 24765:2017	Systems and software engineering – Vocabulary

۵-۳-۳-۱۰- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۸: قابلیت ردیابی، اصل و ریشه (وابستگی به داده‌های گذشته) و شفافیت داده‌ها

Issue 28 — Data transparency, lineage, and traceability	
ANSI INCITS 442	Information Technology – Biometric Identity Assurance Services (BIAS)
ASTM C1009 REV A	Standard Guide for Establishing and Maintaining a Quality Assurance Program for Analytical Laboratories Within the Nuclear Industry
ASTM E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)
ASTM E1931	Standard Guide for Non-computed X-Ray Compton Scatter Tomography
BSI BS 8593	Code of practice for the deployment and use of Body Worn Video (BWV)
BSI PAS 180	Smart cities – Vocabulary
BSI PAS 212	Automatic resource discovery for the Internet of Things – Specification – CORR: November 2016
CGSB CAN/CGSB-72.34	Electronic records as documentary evidence
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ETSI GR PDL 001	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies – V1.1.1
ETSI GS CIM 006	Context Information Management (CIM); Information Model (MOD0) – V1.1.1
ETSI GS CIM 009	Context Information Management (CIM); NGSI-LD API – V1.2.2
ETSI GS INS 005	Identity and access management for Networks and Services; Requirements of an EnforcementFramework in a Distributed Environment – V1.1.1
ETSI GS INS 008	Identity and access management for Networks and Services (INS); Distributed access controlenforcement framework; Architecture – V1.1.1
ETSI TR 103 535	SmartM2M; Guidelines for using semantic interoperability in the industry – V1.1.1
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existingstandardized IoT Platforms — V1.1.2

ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TS 101 533-1	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management — V1.3.1
ISO 16175-2	Information and documentation – Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for digital recordsmanagement systems
ISO 21965	Information and documentation – Records management in enterprise architecture
ISO 25237	Health informatics – Pseudonymization – First Edition
ISO 30401	Knowledge management systems – Requirements.
ISO 5841-2	Implants for Surgery – Cardiac Pacemakers – Part 2 Reporting of Clinical Performance of Populationsof Pulse Generators or Leads
ISO TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap – Part 2: Architecturalcomponents and maturity model – First Edition
ISO TR 19669	Health informatics – Re-usable component strategy for use case development – First Edition
ISO TR 21965	Information and documentation – Records management in enterprise architecture – First edition
ISO TR 22221	Health informatics Good principles and practices for a clinical data warehouse – First Edition
ISO TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care –First Edition
ISO/IEC 19763-1	Information technology – Metamodel framework for interoperability (MFI) Part1: Framework
ISO/IEC 30108-1	Information technology – Biometric Identity Assurance Services – Part 1: BIAS services – First Edition;Corrected version 04-15-2016
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC38500 to the governance of data – First Edition
ISO/IEC TR 16501	Information technology – Generic digital audio-visual systems
ISO/IEC TR 20547-2	Information technology – Big data reference architecture Part 2: Use cases and derived requirements
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence –First edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap – Part 2: Architecturalcomponents and maturity model
ISO/TR 19669	Health informatics – Re-usable component strategy for use case development
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse

ITU-T X.1602	Security requirements for software as aservice application environments — Study Group 17
ITU-T Y.3505	Cloud computing – Overview and functional requirements for data storage federation –Study Group 13
ITU-T Y.3509	Cloud computing – Functional architecture for data storage federation – Study Group 13
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ITU-T Y.4464	(Pre-Published) Framework of blockchain of things as decentralized service platform
SAE PT-186/11	Collision Reconstruction Methodologies Volume 11: Biomechanics – To Purchase Call 1-800-854-7179USA/Canada or 303-397-7956 Worldwide
SNZ AS/NZS 5667.1	Water Quality – Sampling Part 1: Guidance on the Design of Sampling Programs, Sampling Techniquesand the Preservation and Handling of Samples
SNZ NZS 5259	Gas measurement
SNZ SA/SNZ HB 168	Document control
UL 2800 BULLETIN	UL Standard for Safety Medical Device Interoperability – COMMENTS DUE: November 5, 2018
BSI BS 7958 – TC	TC – Tracked Changes (Redline) – Closed circuit television (CCTV) – Management and operation –Code of practice – Compares BS 7958:2015 with BS 7958:2009
CEN EN 9300-002	Aerospace series – LOTAR -LOng Term Archiving and Retrieval of digital technical productdocumentation such as 3D, CAD and PDM data – Part 002: Requirements
ISO 13606-1 – TC	TC – Tracked Changes (Redline) – Health informatics – Electronic health record communication Part 1:Reference model – Compares BS EN ISO 13606-1:2019 with BS EN ISO 13606-1:2012
ISO 21090	Health Informatics – Harmonized data types for information interchange
ISO 13606-1	Health informatics – Electronic health record communication – Part 1: Reference model (ISO 13606-1:2019)
ISO/IEC TR 19583-23	Information technology – Concepts and usage of metadata – Part 23: Data element exchange (DEX)for a subset of ISO/IEC 11179-3 — First Edition
IEEE 2804	Standard for Software-Hardware Interface for Multi-Many-Core – IEEE Computer Society
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ISO/IEC 17913	Information technology – 12,7mm 128-track magnetic tape cartridge for information interchange –Parallel serpentine format
ASTM MNL19	Manual on the Building of Materials Databases
IEEE 1636	Software Interface for Maintenance Information Collection and Analysis (SIMICA)
IEEE 1636.1	Software Interface for Maintenance Information Collection and Analysis (SIMICA): Exchanging TestResults and Session Information via the eXtensible Markup Language (XML)
IEEE 1636.2	Standard for Software Interface for Maintenance Information Collection and Analysis (SIMICA):Exchanging Maintenance Action Information via the Extensible Markup Language (XML)
ISO 22600-1	Health informatics – Privilege management and access control – Part 1: Overview and policy management
ANSI INCITS 315	Information Technology – Magnetic Tape and Cartridge for Information Interchange – Unrecorded,128-Track, Parallel Serpentine, 12.65 mm (1/2 in), 2550 ftpmm (64 770 ftpi)
ISO 10303-232	Industrial Automation Systems and Integration – Product Data Representation and Exchange – Part232: Application Protocol: Tehcnical Data Packaging Core Information

	and Exchange – First Edition
CEN/TR 16742	Intelligent transport systems – Privacy aspects inITS standards and systems inEurope
CSA Z8002-14	Operation and maintenance of health care facilities – Second edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
IEEE Std 1857.6-2018	IEEE Standard for Digital Media Content Description
CSA Z8003	Health care design research and evaluation

۵-۳-۳-۱۱- استانداردهای دسترسی به داده‌ها و اشتراک‌گذاری و نگهداری آن‌ها _ موضوع ۲۹: قابلیت جابه‌جایی و حمل داده‌ها

Issue 29 — Data portability and mobility	
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI PAS 1040	Digital readiness – Adopting digital technologies in manufacturing – Guide
BSI PAS 1085	Manufacturing – Establishing and implementing a security-minded approach – Specification
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and informationservices
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach –CORR: May 30, 2018
BSI PAS 1885	The fundamental principles of automotive cyber security – Specification
BSI PAS 201	Supporting fintechs in engaging with financial institutions – Guide
BSI PAS 92	Code of practice for the implementation of a biometric system
BSI PD CEN/TR 16931-4	Electronic invoicing Part 4: Guidelines on interoperability of electronic invoices at thetransmission level
BSI PD CEN/TR 17143	Intelligent transport systems – Standards and actions necessary to enable urban infrastructurecoordination to support Urban-ITS
BSI PD CEN/TR 17475	Space – Use of GNSS-based positioning for road Intelligent Transport System (ITS) – Specification of the test facilitities, definition of test scenarios,description and validation of the procedures for fieldtest related to security performance of GNSS-based positioning terminals

BSI PD CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
CEN EN 16234-1	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in allsectors Part 1: Framework
CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
CSA CSA-Q830-03	Model Code for the Protection of Personal Information – Second Edition
DIN SPEC 4997	Privacy by Bbckchain Design: Astandardised model for processing personal data using blockchaintechnology; Text in English
DIN SPEC 91347	Integrated multi-functional Humble Lamppost (mHLa)
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
DIN SPEC 91367	Urban mobility data collection for real-time applications; Text in English
DIN SPEC 91406	Automatic identification of physical objects and information on physical objects in IT systems,particularly IoT systems; Text in German and English
DS DS/CEN/TR 17439	Guidance on how to implement EN ISO 19650-1 and -2 in Europe
DS DS/CEN/TR 17475	Space – Use of GNSS-based positioning for road Intelligent Transport System (ITS) – Specification of the test facilities, definition of test scenarios, description and validation of the procedures for fieldtests related to security performance of GNSS-based positioning terminals
DS DS/CWA 16871-1	Requirements and Recommendations for Assurance inCloud Security – Part 1: Contributedrecommendations from European projects
EN 319 531	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for RegisteredElectronic Mail Service Providers — V1.1.1
EN 319 532-1	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1:Framework and architecture — V1.1.1
EN 319 532-2	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2:Semantic contents — V1.1.1
ETSI GR CIM 002	Context Information Management (CIM); Use Cases (UC) – V1.1.1
ETSI GR ENI 007	Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application toNetworks — V1.1.1
ETSI GR PDL 001	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies – V1.1.1
ETSI GR ZSM 004	Zero-touch network and Service Management (ZSM); Landscape – V1.1.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and RegulatoryConcerns — V1.1.1
ETSI SR 003 381	Cloud Standards Coordination Phase 2; Identification of Cloud user needs – V2.1.1
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI SR 003 392	Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; Anewsnapshot of Cloud Computing Standards – V2.1.1
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A ConcreteApproach — V1.1.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 477	eHEALTH; Standardization use cases for eHealth – V1.1.1

ETSI TR 103 509	SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well – V1.1.1
ETSI TR 103 533	SmartM2M; Security; Standards Landscape and best practices – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existingstandardized IoT Platforms — V1.1.2
ETSI TR 103 582	EMTEL; Study of use cases and communications involving IoT devices in provision of emergencysituations — V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TR 119 500	Business Driven Guidance for Trust Application Service Providers – V1.1.1
ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT) – V15.3.0; Release 15
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoTdevices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
ETSI TS 103 643	Techniques for assurance of digital material used in legal proceedings – V1.1.1
ETSI TS 132 421	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile TelecommunicationsSystem (UMTS); LTE; Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements – V15.3.0; 3GPP TS 32.421 version 15.3.0 Release 15
IEC 61800-7-202	Adjustable speed electrical power drive systems – Part 7-202: Generic interface and use of profilesfor power drive systems – Profile type 2 specification – Edition 2.0
IEEE 1900 SERIES	Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging WirelessNetworks, System Functionality, and Spectrum Management – Includes IEEE 1900.1, IEEE 1900.2, IEEE 1900.4, IEEE 1900.4a, IEEE 1900.4.1, IEEE 1900.5, IEEE 1900.5.2, IEEE 1900.6, IEEE 1900.6A, IEEE 1900.7
IEEE 1934	Adoption of OpenFog Reference Architecture for Fog Computing
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on HumanWell-Being
IEEE NEUROTECHNOLOGIES BMI ROADMAP	STANDARDS ROADMAP: NEUROTECHNOLOGIES FOR BRAIN-MACHINE INTERFACING
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	PHD Cybersecurity Standards Roadmap – Version: 1.0
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 10617	Textiles – Standard data format for colorimetric communication – Textiles and related measurements
ISO 10667-2	Assessment service delivery – Procedures and methods to assess people in work and organizationalsettings Part 2: Requirements for service providers
ISO 13606-4	Health informatics – Electronic health record communication – Part 4: Security – First edition
ISO 17115	Health informatics – Representation of categorial structures of terminology

	(CatStructure)
ISO 17117-1	Health informatics – Terminological resources – Part 1: Characteristics
ISO 18308	Health informatics – Requirements for an electronic health record architecture
ISO 18750	Intelligent transport systems – Co-operative ITS – Local dynamic map (ISO 18750:2018)
ISO 19465	Traditional Chinese medicine – Categories of traditional Chinese medicine (TCM) clinicalterminological systems
ISO 19626-1	Processes, data elements and documents in commerce, industry and administration – Trustedcommunication platforms for electronic documents Part 1: Fundamentals
ISO 20264	Stationary source emissions – Determination of the mass concentration of individual volatile organiccompounds (VOCs) in waste gases from non-combustion processes – First edition
ISO 22367	Medical laboratories – Application of risk management to medical laboratories – CORR: May 31, 2020
ISO 23354	Business requirements for end-toend visibility of logistics flow
ISO 25237	Health informatics – Pseudonymization – First Edition
ISO 26000	Guidance on social responsibility (ISO 26000:2010)
ISO 37156	Smart community infrastructures – Guidelines on data exchange and sharing for smart communityinfrastructures
ISO IWA 31	Risk management – Guidelines on using ISO 31000 in management systems
ISO TR 24971	Medical devices — Guidance on the application of ISO 14971 — Second edition (STANDARDPLUS REDLINE)
ISO TS 16843-1	Health informatics – Categorial structures for representation of acupuncture – Part 1: Acupuncturepoints — First Edition
ISO TS 16843-2	Health informatics – Categorial structures for representation of acupuncture – Part 2: Needling –First Edition
ISO TS 16843-3	Health informatics – Categorial structures for representation of acupuncture – Part 3: Moxibustion –First Edition
ISO TS 16843-4	Health informatics – Categorial structures for representation of acupuncture – Part 4: Meridian andcollateral channels — First Edition
ISO TS 16843-5	Health Informatics – Categorial structures for representation of acupuncture – Part 5: Cupping –First Edition
ISO TS 18101-1	Automation systems and integration – Oil and gas interoperability – Part 1: Overview and fundamentalprinciples — First edition
ISO TS 18790-1	Health informatics – Profiling framework and classification for Traditional Medicine informaticsstandards development – Part 1: Traditional Chinese Medicine – First Edition
ISO TS 19299	Electronic fee collection – Security framework – First Edition
ISO TS 19844	Health informatics – Identification of medicinal products (IDMP) – Implementation guidelines for ISO 11238 for data elements and structures for the unique identification and exchange of regulatedinformation on substances — Third Edition
ISO TS 21192	Electronic fee collection – Support for traffic management – First edition
ISO TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles –First Edition
ISO TS 21831	Information model of Chinese materia medica processing – First edition
ISO TS 22773	Health Informatics – Categorial structures for the representation of the decocting process intraditional Chinese medicine – First edition

ISO TS 22789	Health informatics – Conceptual framework for patient findings and problems in terminologies –First Edition
ISO TS 22835	Health informatics – Information model of combination of decoction pieces in Chinese medicines –First Edition
ISO TS 22990	Traditional Chinese medicine – Categories of clinical terminological system to support the integrationof clinical terms from traditional Chinese medicine and Western medicine – First edition
ISO TS 23303	Health informatics – Categorial structure for Chinese materia medica products manufacturingprocess — First edition
ISO TS 8000-311	Data quality – Part 311: Guidance for the application of product data quality for shape (PDQ-S) –First Edition
ISO/IEC 12087-5	Information technology Computer graphics and image processing Image Processing and Interchange(IPI) Functional specification Part 5: Basic Image Interchange Format (BIIF)
ISO/IEC 15944-12	Information technology — Business operational view Part 12: Privacy protection requirements (PPR) oninformation life cycle management (ILCM) and EDI of personal information (PI)
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture (ISO/IEC 17789:2014)
ISO/IEC 18384-2	Information technology – Reference Architecture for Service Oriented Architecture (SOA RA) – Part 2:Reference Architecture for SOA Solutions – First Edition
ISO/IEC 19086-1	Information technology – Cloud computing – Service level agreement (SLA) framework Part 1:Overview and concepts
ISO/IEC 19086-3	Information technology – Cloud computing – Service level agreement (SLA) framework Part 3: Coreconformance requirements
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services –First Edition
ISO/IEC 19780-1	Information technology – Learning, education and training – Collaborative technology – Collaborativelearning communication – Part 1: Text-based communication
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categoriesand data use — First Edition
ISO/IEC 20748.2	Information technology for learning, education and training – Learning analytics interoperability Part 2:System requirements
ISO/IEC 21964-1	Information technology – Destruction of data carriers Part 1: Principles and definitions
ISO/IEC 21964-3	Information technology – Destruction of data carriers Part 3: Process of destruction of data carriers
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services –First edition
ISO/IEC 27701	Expert commentary BS ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 andISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC 29184	Information technology – Online privacy notices and consent
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC GUIDE 71	Guide for addressing accessibility in standards
ISO/IEC TR 20547-2	Information technology – Big data reference architecture Part 2: Use cases and derived requirements
ISO/IEC TR 20748-2	Information technology for learning, education and training – Learning analytics

	interoperability Part 2:System requirements – CORR: August 31, 2018
ISO/IEC TR 22678	Information technology – Cloud computing – Guidance for policy development
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC38505-1 for data management
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO/IEC/IEEE 8802-1AX	Information technology – Telecommunications and information exchange between systems – Localand metropolitan area networks – Specific requirements Part 1AX: Link Aggregation – First Edition
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/TR 23021	Traditional Chinese medicine – Controlled vocabulary on Japanese Kampo crude drugs
ISO/TR 23022	Traditional Chinese medicine – Controlled vocabulary on Japanese Kampo formulas and theindication codes for the products
ISO/TR 24971	Medical devices – Guidance on the application of ISO 14971
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformityassessment – CORR: February 28, 2014
ISO/TS 16277-1	Health informatics – Categorial structures of clinical findings in traditional medicine Part 1: TraditionalChinese, Japanese and Korean medicine
ISO/TS 16843-1	Health informatics – Categorial structures for representation of acupuncture – Part 1: Acupuncture points
ISO/TS 16843-3	Health informatics – Categorial structures for representation of acupuncture Part 3: Moxibustion
ISO/TS 16843-4	Health informatics – Categorial structures for representation of acupuncture Part 4: Meridian andcollateral channels
ISO/TS 16843-5	Health Informatics – Categorial structures for representation of acupuncture – Part 5: Cupping
ISO/TS 18062	Health informatics – Categorial structure for representation of herbal medicaments in terminological systems
ISO/TS 18101-1	Automation systems and integration – Oil and gas interoperability – Part 1: Overview andfundamental principles
ISO/TS 18750	Intelligent transport systems – Cooperative systems – Definition of a global concept for LocalDynamic Maps (ISO/TS 18750:2015); English version CEN ISO/TS 18750:2015
ISO/TS 18790-1	Health informatics – Profiling framework and classification for Traditional Medicine informaticsstandards development Part 1: Traditional Chinese Medicine
ISO/TS 21192	Electronic fee collection – Support for traffic management
ISO/TS 21564	Health Informatics – Terminology resource map quality measures (MapQual)
ISO/TS 21831	Information model of Chinese materia medica processing
ISO/TS 22773	Health Informatics – Categorial structures for the representation of the decocting process intraditional Chinese medicine
ISO/TS 22835	Health informatics – Information model of combination of decoction pieces in Chinese medicines

ISO/TS 23303	Health informatics – Categorial structure for Chinese materia medica products manufacturing process
ITU-R M.1457-14	Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)
ITU-T G.1032	(Pre-Published) Influence Factors on Gaming Quality of Experience
ITU-T K.81	High-power electromagnetic immunity guide for telecommunication systems – Study Group 5
ITU-T L.1305	Data centre infrastructure management system based on big data and artificial intelligencetechnology — Study Group 5
ITU-T L.1470	Greenhouse gas emissions trajectories for the information and communication technology sectorcompatible with the UNFCCC Paris Agreement – Study Group 5
ITU-T SERIES H SUPP 17	Guide for addressing accessibility in standards – Study Group 16
ITU-T SERIES Q SUPP 65	Cloud computing interoperability activities – Study Group 11
ITU-T SERIES Q SUPP 66	Supplement on scenarios and requirements in terms of services and deployments for IMT and IMS indeveloping countries — Study Group 13
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T SERIES Y SUPP 52	Methodology for building digital capabilities during enterprises' digital transformation – StudyGroup 20
ITU-T SERIES Y SUPP 56	ITU-T Y-series – Supplement on use cases of smart cities and communities – Study Group 20
ITU-T Y.3052	Overview of trust provisioning in information and communication technology infrastructures andservices — Study Group 13
ITU-T Y.3173	Framework for evaluating intelligence levels of future networks including IMT-2020 – Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ITU-T Y.4003	Overview of smart manufacturing in the context of the industrial Internet of things – Study Group 20
ITU-T Y.4905	(Pre-Published) Smart sustainable city impact assessment
ITU-T Y.4906	Assessment framework for digital transformation of sectors in smart cities – Study Group 20
SAE AIR6904	Rationale, Considerations, and Framework for Data Interoperability for Health Management within theAerospace Ecosystem
SAE AS5506C	(R) Architecture Analysis & Design Language (AADL)
SAE R-463	Introduction to Advanced Manufacturing – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CSA Z8003	Health care design research and evaluation

۵-۳-۴- استانداردهای مرتبط با کارگروه ۴: تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها

۵-۳-۴-۱- استانداردهای تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها _ موضوع ۳۰: مؤلفه‌های فنی راه حل‌های هوش مصنوعی

Issue 30 — Technical Elements of AI Solutions	
ANSI INCITS 172	Information Technology – American National Standard Dictionary of Information Technology (ANSDIT)
ANSI X9.112-3	Wireless Management and Security Part 3: Mobile
API PUBL 4452	1987 Oil Spill Conference
ASCE 70-19	Estimation of Aquifer Hydraulic Properties by Inverse Numerical Modeling of Aquifer Pumping Tests
ASCE GSP 199	GEOFLORIDA 2010 ADVANCES IN ANALYSIS, MODELING & DESIGN
ASCE GSP 318	Geo-Congress 2020: Geotechnical Earthquake Engineering and Special Topics
ASHRAE 4692	Development and Implementation of HVAC-KBCD: A Knowledge-Based Expert System forConceptual Design of HVAC&R System – Part 2: Application to Office Buildings
ASHRAE AB-10-022	To Assess the Validity of the Transfer Function Method: A Neural Model for the Optimal Choice ofConduction Transfer Functions
ASHRAE DATACOM SERIES BOOK 14	Advancing DCIM with IT Equipment Integration
ASHRAE TRAN 2010-2	2010 ASHRAE TRANSACTIONS VOLUME 116 PART 2
ASHRAE TRAN 2019-2	2019 ASHRAE TRANSACTIONS – VOLUME 125, PART 2
ASHRAE TRAN 2020-1	2020 ASHRAE TRANSACTIONS – VOLUME 126 – PART 1
ASTM F2446	Standard Classification for Hierarchy of Equipment Identifiers and Boundaries for Reliability, Availability,and Maintainability (RAM) Performance Data Exchange
ASTM F3060	Standard Terminology for Aircraft
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code ofpractice for implementation of BS 10008-1
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI BS 5192-1	Guide to Production Control – Part 1: Introduction

BSI PAS 1000	Business agility – Concept and framework – Guide
BSI PAS 1040	Digital readiness – Adopting digital technologies in manufacturing – Guide
BSI PAS 1085	Manufacturing – Establishing and implementing a security-minded approach – Specification
BSI PAS 1880	Guidelines for developing and assessing control systems for automated vehicles – FREE DOWLOANDFROM BSI SHOP
BSI PAS 1885	The fundamental principles of automotive cyber security – Specification
BSI PAS 440	Responsible innovation – Guide
BSI PAS 7040	Digital manufacturing – Trustworthiness and precision of networked sensors – Guide
BSI PAS 7340	Framework for embedding the principles of sustainable fi nance in fi nancial servicesorganizations — Guide
CIE X046 VOL 1-2	PROCEEDINGS of the 29th Session of the CIE Washington D.C., USA, June 14 – 22, 2019Volume 1 — Part 2
DS DS/CWA 17492	Predictive control and maintenance of data intensive industrial processes
DIN SPEC 92001-1	Artificial Intelligence – Life Cycle Processes and Quality Requirements – Part 1: Quality Meta Model;Text in English
ETSI EG 202 301	Universal Communications Identifier (UCI); Using UCI to enhance communications for disabled, youngand elderly people — V1.1.1
ETSI EN 303 470	Environmental Engineering (EE); Energy Efficiency measurement methodology and metrics forservers — V1.1.1
ETSI ES 202 336-12	Environmental Engineering (EE); Monitoring and control interface for infrastructure equipment (power, cooling and building environment systems used in telecommunication networks); Part 12: ICTequipment power, energy and environmental parameters monitoring information model — V1.2.1
ETSI GR ARF 002	Augmented Reality Framework (ARF) Industrial use cases for AR applications and services – V1.1.1
ETSI GR CIM 002	Context Information Management (CIM); Use Cases (UC) – V1.1.1
ETSI GR ENI 003	Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis – V1.1.1
ETSI GR ENI 004	Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI – V2.1.1
ETSI GR ENI 007	Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application toNetworks — V1.1.1
ETSI GR ZSM 004	Zero-touch network and Service Management (ZSM); Landscape – V1.1.1
ETSI GS ENI 001	Experiential Networked Intelligence (ENI); ENI use cases – V2.1.1
ETSI GS ENI 002	Experiential Networked Intelligence (ENI); ENI requirements – V2.1.1
ETSI GS ENI 005	Experiential Networked Intelligence (ENI); System Architecture – V1.1.1
ETSI GS MEC 002	Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements – V2.1.1
ETSI GS ZSM 001	Zero-touch network and Service Management (ZSM); Requirements based on documentedscenarios — V1.1.1

ETSI GS ZSM 002	Zero-touch network and Service Management (ZSM); Reference Architecture – V1.1.1
ETSI GS ZSM 007	Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM – V1.1.1
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A ConcreteApproach — V1.1.1
ETSI TR 102 647	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Management; Operation Support System Standards Overview and Gap Analysis —V1.2.1; Includes Diskette
ETSI TR 102 659-1	GRID; Study of ICT Grid interoperability gaps; Part 1: Inventory of ICT Stakeholders – V1.2.1
ETSI TR 103 077	Universal Communications Identifier (UCI); Maximizing the Usability of UCI Based Systems – V1.1.1
ETSI TR 103 306	CYBER; Global Cyber Security Ecosystem – V1.4.1
ETSI TR 103 438	User Group; User centric approach in Digital Ecosystem – V1.1.1; Includes Diskette
ETSI TR 103 508	SmartM2M; SAREF extension investigation; Requirements for Automotive – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existingstandardized IoT Platforms — V1.1.2
ETSI TR 103 562	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Analysis ofthe Collective Perception Service (CPS); Release 2 – V2.1.1
ETSI TR 103 582	EMTEL; Study of use cases and communications involving IoT devices in provision of emergencysituations — V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TR 103 626	Autonomic network engineering for the self-managing Future Internet (AFI); An Instantiation and Implementation of the Generic Autonomic Network Architecture (GANA) Model onto HeterogeneousWireless Access Technologies using Cognitive Algorithms – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TS 103 195-2	Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2 An Architectural Reference Model for Autonomic Networking, CognitiveNetworking and Self-Management — V1.1.1
ETSI TS 103 300-2	Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 2: FunctionalArchitecture and Requirements definition – V2.1.1; Release 2
ETSI TS 105 174-8	Access, Terminals, Transmission and Multiplexing (ATTM); Broadband Deployment and LifecycleResource Management; Part 8Implementation of WEEE practices for ICT equipment during maintenance and at end-of-life — V1.2.1
IEC 60050-171	International Electrotechnical Vocabulary (IEV) – Part 171: Digital technology – Fundamentalconcepts — Edition 1.0

IEC 60194	Printed board design, manufacture and assembly – Terms and definitions
IEC 61508 SET REDLINE	Functional Safety of Electrical/Electronic/programmable Electronic Safety – Related Systems Set *** Contains IEC 61508-1 Through IEC 61508-7*** – Edition 2.0; ***NOT AVAILABLE FOR CUSTOMCOLLECTIONS AT THIS TIME*** All Retail Customer Must Purchase the DVD
IEC 61508-7	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7:Overview of techniques and measures – Edition 2.0
IEC 62243	Artificial intelligence exchange and service tie to all test environments (AI-ESTATE)
IEEE 1484.1	IEEE Standard for Learning TechnologyLearning Technology Systems Architecture (LTSA) – IEEEComputer Society
IEEE 1636	Software Interface for Maintenance Information Collection and Analysis (SIMICA)
IEEE 1671.1	Automatic Test Markup Language (ATML) Test Descriptions
IEEE 1900 SERIES	Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging WirelessNetworks, System Functionality, and Spectrum Management – Includes IEEE 1900.1, IEEE 1900.2, IEEE 1900.4, IEEE 1900.4a, IEEE 1900.4.1, IEEE 1900.5, IEEE 1900.5.2, IEEE 1900.6, IEEE 1900.6A, IEEE 1900.7
IEEE 1900.1	Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging WirelessNetworks, System Functionality, and Spectrum Management
IEEE 1934	Adoption of OpenFog Reference Architecture for Fog Computing
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 2430	Trial-Use Standard for Software Non-Functional Sizing Measurements – IEEE Computer Society
IEEE 24765	Systems and software engineering – Vocabulary – IEEE Computer Society
IEEE 2755.1	Guide for Taxonomy for Intelligent Process Automation Product Features and Functionality
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on HumanWell-Being
IEEE 802.22	Information Technology – Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN) – Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the Bands that Allow Spectrum Sharing where the Communications Devices May Opportunistically Operate in the Spectrum of Primary Service – IEEE Computer Society
IEEE NEUROTECHNOLOGIES BMI ROADMAP	STANDARDS ROADMAP: NEUROTECHNOLOGIES FOR BRAIN-MACHINE INTERFACING

IEEE WHITE PAPER 3DBP IC	IEEE 3D BODY PROCESSING INDUSTRY CONNECTIONS (3DBP IC): COMMUNICATION, SECURITY,AND PRIVACY
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 16355-3	Applications of statistical and related methods to new technology and product development process Part 3: Quantitative approaches for the acquisition of voice of customer and voice of stakeholder
ISO 24617-1	Language resource management – Semantic annotation framework (SemAF) – Part 1: Time andevents (SemAF-Time, ISO-TimeML)
ISO 24617-7	Language resource management – Semantic annotation framework Part 7: Spatial information
ISO 9409-1	Manipulating industrial robots – Mechanical interfaces – Part 1: Plates
ISO IWA 31	Risk management – Guidelines on using ISO 31000 in management systems
ISO TR 23455	Blockchain and distributed ledger technologies – Overview of and interactions between smartcontracts in blockchain and distributed ledger technology systems – First edition
ISO/IEC 11179-1	Information technology – Specification and standardization of data elements – Part 1: Framework forthe specification and standardization of data elements
ISO/IEC 19788-3	Information technology – Learning, education and training – Metadata for learning resources – Part 3:Basic application profile AMENDMENT 1
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO/IEC 23001-4	Information technology – MPEG systems technologies – Part 4: Codec configuration representation
ISO/IEC 2382-1	Information technology – Vocabulary – Part 1: Fundamental terms
ISO/IEC 27021	Information technology – Security techniques – Competence requirements for information securitymanagement systems professionals
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC TR 24741	Information technology – Technical Report for a Biometrics Tutorial (Technical Report)
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes –First edition
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4:Privacy and data protection policies
ISO/TR 23455	Blockchain and distributed ledger technologies – Overview of and interactions between smartcontracts in blockchain and distributed ledger technology systems
ISO/TR 23845	Biomimetics – Ontology-Enhanced Thesaurus (OET) for biomimetics
ISO/TS 22287	Health informatics – Workforce roles and capabilities for terminology and terminology services inhealthcare (term workforce)

ITU-T F.749.10	Requirements for communication services of civilian unmanned aerial vehicles – Study Group 16
ITU-T L.1022	Circular economy: Definitions and concepts for material efficiency for information and communicationtechnology — Study Group 5
ITU-T L.1305	Data centre infrastructure management system based on big data and artificial intelligence technology — Study Group 5
ITU-T L.1380	Smart energy solution for telecom sites – Study Group 5
ITU-T M.3041	Framework of smart operation, management and maintenance – Study Group 2
ITU-T Q.1200	General Series Intelligent Network Recommendation Structure – Series Q: Switching and Signalling –Intelligent Network — Study Group 11; 11 pp
ITU-T SERIES K SUPP 16	Electromagnetic field compliance assessments for 5G wireless networks – Study Group 5
ITU-T Y.3101	Requirements of the IMT-2020 network – Study Group 13
ITU-T Y.3173	Framework for evaluating intelligence levels of future networks including IMT-2020 – Study Group 13
ITU-T Y.3324	Requirements and architectural framework for autonomic management and control of IMT-2020networks — Study Group 13
ITU-T Y.3508	Cloud computing – Overview and high-level requirements of distributed cloud – Study Group 13
ITU-T Y.3800	Overview on networks supporting quantum key distribution – Study Group 13
ITU-T Y.4003	Overview of smart manufacturing in the context of the industrial Internet of things – Study Group 20
ITU-T Y.4204	Accessibility requirements for the Internet of things applications and services – Study Group TSAG
ITU-T Y.4904	Smart sustainable cities maturity model – Study Group 20
ITU-T Y.4906	Assessment framework for digital transformation of sectors in smart cities – Study Group 20
NEMA IOT P2	A NEMA White Paper on Emerging Technologies and the Industrial Internet of Things andTheir Applications
SAE AIR1266A	Fault Isolation in Environmental Control Systems of Commercial Transports
SAE ARP5150A	(R) Safety Assessment of Transport Airplanes in Commercial Service
SAE ARP6407	IVHM Design Guidelines
SAE PT-202	Material and Process Modeling of Aerospace Composites – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide

SAE PT-204	Multi-Agent Safety: Book 2 – Automated Vehicle Safety – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SAE PT-205	Safety of the Intended Functionality: Book 3 – Automated Vehicle Safety – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SAE PT-207	The Safety of Controllers, Sensors, and Actuators: Book 5 – Automated Vehicle Safety – To PurchaseCall 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SAE R-441	No Fault Found: The Search for the Root Cause – To Purchase Call 1-800-854-7179 USA/Canada or303-397-7956 Worldwide
SAE R-463	Introduction to Advanced Manufacturing – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
UL 4600	UL STANDARD FOR SAFETY Evaluation of Autonomous Products – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
IMDRF/SaMD WG/ N10FINAL:201	Software as a Medical Device (SaMD): Key Definitions (IMDRF/SaMD WG/N10FINAL:2013)
IMDRF/SaMD WG/ N12FINAL:2014	Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and CorrespondingConsiderations (IMDRF/SaMD WG/N12FINAL:2014)
IMDRF/SaMD WG/N23 FINAL:2015	Software as a Medical Device (SaMD): Application of Quality Management System (IMDRF/SaMD WG/N23 FINAL:2015)
N/A	Guidance Document: Software as a Medical Device (SaMD): Definition and Classification
N/A	Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback
ISO/IEC DTR 29119-11	Software and systems engineering – Software testing – Part 11: Testing of AI-based systems
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
CAN/CIOSC 107	Testing and proving grounds for autonomous vehicles
IEEE P1232.3/D3.2	IEEE Approved Draft Guide for the Use of Artificial Intelligence Exchange and Service Tie to All TestEnvironments (AI-ESTATE)

۵-۳-۴-۲- استانداردهای تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها _ موضوع ۳۱: زنجیره ارزش داده‌ها

Issue 31 — Data value chain	
ETSI TR 103 376	SmartM2M; IoT LSP use cases and standards gaps – V1.1.1
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
IEEE 1232.1	Trial Use – Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments(AI-ESTATE): Data and Knowledge Specification

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
N/A	Realising the value of health care data: a framework for the future
N/A	Study: The value of data in Canada: Experimental estimates
N/A	Competence Center Corporate Data Quality (CC CDQ)
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
IEEE IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

۵-۳-۴-۳- استانداردهای تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها _ موضوع ۳۲: شفافیت و ارتباط تجزیه‌وتحلیل داده‌ها

Issue 32 —Transparency and communication of data analytics	
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
n/a	Datasheets for Datasets
n/a	Public Opinion Research Standards and Disclosure Requirements
n/a	A privacy-preserving data cloud for health care
ISO/IEC 20889:2018	Privacy enhancing data de-identification terminology and classification of techniques
n/a	The value of ashared understanding ofAI models

n/a	Explainable Artificial Intelligence (XAI)
n/a	Regulation (EU) 2016/679 of the European Parliament and the Council – on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, andrepealing Directive 95/46/EC (General Data Protection Regulation)
n/a	Algorithmic Impact Assessment (AIA)
n/a	Open Data
n/a	Designing for Digital Transparency in the Public Realm
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
IEEE P7001	IEEE Draft Standard for Transparency of Autonomous Systems
IEEE IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

۵-۳-۴-۴- استانداردهای تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها _ موضوع ۳۳: تفسیرپذیری و توضیح‌پذیری سیستم‌های هوش مصنوعی (تفسیرپذیری الگوریتم‌ها)

Issue 33 — Interpretability and explainability of AI systems (Originally "Interpretability of algorithms.)	
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
n/a	Explainable Artificial Intelligence (XAI)
n/a	Ethics Guidelines for Trustworthy AI
n/a	Regulation (EU) 2016/679 of the European Parliament and the Council – on the protection of naturalpersons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
ISO/IEC DTR 29119-11	Software and systems engineering – Software testing – Part 11: Testing of AI-based systems
n/a	White Paper on Artificial Intelligence – A European approach to excellence and trust
ISO/IEC TR 24028:2020	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence
n/a	Data Ethics Canvas
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
IEEE P2894	Guide for an Architectural Framework for Explainable Artificial Intelligence

۵-۳-۴-۵- استانداردهای تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها _ موضوع ۳۴: ارزیابی و مدیریت سوگیری (غرض‌ورزی)

Issue 34 — Assessment and management of bias	
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/IEC AWI TR 24027	Information technology – Artificial Intelligence (AI) – Bias in AI systems and AI aided decision making
IEEE P7003	Algorithmic Bias Considerations
n/a	Ethical Guidelines for Statistical Practice
n/a	The Data Equity Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoringdata in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
IEEE P7003	Algorithmic Bias
N/A	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

۵-۳-۴-۶- استانداردهای تجزیه‌وتحلیل داده‌ها، نوآوری و تجاری‌سازی آن‌ها _ موضوع ۳۵: سیستم‌های مدیریت کارایی برای سیستم‌های هوش مصنوعی و تجزیه‌وتحلیل

Issue 35 — Performance management systems for analytics and AI systems	
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/IEC 38507	Information technology – Governance of IT – Governance implications of the use of artificial intelligenceby organizations
n/a	Ethical Dimensions of Using Artificial Intelligence in Health Care
n/a	ISO MANAGEMENT SYSTEM STANDARDS (MSS)
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada

۶- پیشنهادات

از آن جایی که موضوعات و حوزه‌های مرتبط با حکمرانی داده بسیار گسترده هستند لازم است در ابتدا اولویت‌بندی از موضوعات مهم مرتبط با صنعت آب و برق ارائه شود و سپس برای هر یک از موضوعات مطرح در حکمرانی داده، استانداردهای مرتبط موجود و در حال تدوین با هر موضوع و قابل به کارگیری در صنعت آب و برق مشخص و نکات کلیدی آن‌ها در قالب دستورالعمل مشخص شود. سپس چالش‌ها و وضعیت داده‌ها در هر یک از موضوعات مطرح مورد تحلیل قرار گیرد و گزارشات مربوطه ارائه شود. همچنین خاطرنشان می‌گردد گام‌های مربوط به آزادسازی داده و اطلاعات اولیه مورد نیاز برای جمع‌آوری دیتاست‌های صنعت آب و برق با استناد به استاندارد چارچوب داده باز در شهرهای هوشمند و مطالعات الگوبرداری در گزارش دیگری ارائه شده است.

۷- مراجع

[1] Recommendation Y.4461 ITU-T: Framework of open data in smart cities. Available on: https://www.itu.int/rec/T-REC-Y.4461-202001-I/en

[2] فناوری اطلاعات- حکمرانی فناوری اطلاعات- حکمرانی داده‌ها، قسمت ۱: کاربرد استاندارد ISO/IEC 38500 در حکمرانی داده‌ها، سازمان ملی استاندارد ایران. قابل دسترسی از: https://standard.inso.gov.ir/

[3] Technical report ISO/IEC TR 38505-2: Information Technology-Governance of IT- Governance of data- Part 2: Implications of ISO/IEC 38505-1 for data management. Available on: https://www.iso.org/standard/70911.html

[4] Standars Council of Canada, “Canadian Data Governance Standardization Roadmap,” 2021. Available on: https://www.scc.ca/en/system/files/publications/SCC_Data_Gov_Roadmap_EN.pdf