TCVN T I Ê U C H U Ẩ N Q U Ố C G I A

**TCVN ISO/IEC 20547-4:2022**

**ISO/IEC 20547-4:2020**

**CÔNG NGHỆ THÔNG TIN –**

**KIẾN TRÚC THAM CHIẾU DỮ LIỆU LỚN –**

**PHẦN 4: BẢO MẬT VÀ QUYỀN RIÊNG TƯ**

***Information technology - Big data reference architecture –***

***Part 4: Security and privacy***

**HÀ NỘI - 2022**

**Mục lục**

[1. Phạm vi áp dụng 4](#_Toc122943688)

[2. Tài liệu viện dẫn 4](#_Toc122943689)

[3. Thuật ngữ và định nghĩa 4](#_Toc122943690)

[4. Chữ viết tắt 4](#_Toc122943691)

[5. Tổng quan 5](#_Toc122943692)

[5.1. Các mối quan tâm về tính bảo mật và quyền riêng tư dữ liệu lớn 5](#_Toc122943693)

[5.2. Mục tiêu bảo mật và quyền riêng tư 8](#_Toc122943694)

[6. Khía cạnh bảo mật và quyền riêng tư của BRDA góc nhìn người dùng 10](#_Toc122943695)

[6.1. Hoạt động quản trị 10](#_Toc122943696)

[6.1.1. Mục đích 10](#_Toc122943697)

[6.1.2. Chuẩn bị và lập kế hoạch cho nỗ lực quản trị BD S&P 11](#_Toc122943698)

[6.1.3. Giám sát, đánh giá và kiểm soát các hoạt động quản trị BD-S&P 11](#_Toc122943699)

[6.1.4. Thiết lập các mục tiêu quản trị BD-S&P 12](#_Toc122943700)

[6.1.5. Chỉ đạo BD-S&P 13](#_Toc122943701)

[6.1.6. Theo dõi và đánh giá sự tuân thủ với các chỉ thị và hướng dẫn quản trị BD-S&P 13](#_Toc122943702)

[6.1.7. Rà soát thực hiện các hướng dẫn và chỉ thị quản trị BD-S&P và chuẩn bị cho thay đổi……. 14](#_Toc122943703)

[6.2. Các hoạt động quản lý 14](#_Toc122943704)

[6.2.1. Mục đích 14](#_Toc122943705)

[6.2.2. Chuẩn bị và lên kế hoạch cho nỗ lực quản trị BD-S&P 14](#_Toc122943706)

[6.2.3. Giám sát, đánh giá và kiểm soát các hoạt động quản lý kiến trúc 15](#_Toc122943707)

[6.2.4. Xây dựng cách tiếp cận quản lý BD-S&P 15](#_Toc122943708)

[6.2.5. Thực hiện quản lý BD-S&P 16](#_Toc122943709)

[6.2.6. Giám sát tính hiệu quả của BD-S&P 17](#_Toc122943710)

[6.2.7. Cập nhật kế hoạch quản lý BD-S&P 18](#_Toc122943711)

[6.3. Hoạt động vận hành 18](#_Toc122943712)

[6.3.1. Hoạt động thiết kế giải pháp BD-S&P 18](#_Toc122943713)

[6.3.2. Các hoạt động đánh giá giải pháp BD-S&P 23](#_Toc122943714)

[6.3.3. Các hoạt động hỗ trợ giải pháp BD-S&P 29](#_Toc122943715)

[6.4. Các khía cạnh bảo mật và quyền riêng tư của các vai trò dữ liệu lớn 32](#_Toc122943716)

[7. Hướng dẫn về các hoạt động bảo mật và quyển riêng tư cho dữ liệu lớn 35](#_Toc122943717)

[7.1. Khái quát chung 35](#_Toc122943718)

[7.2. Hướng dẫn ở mức tổ chức 37](#_Toc122943719)

[7.2.1. Khái quát chung 37](#_Toc122943720)

[7.2.2. Hướng dẫn tiêu chuẩn cho các yêu cầu 38](#_Toc122943721)

[7.2.3. Hướng dẫn tiêu chuẩn cho quản lý rủi ro 39](#_Toc122943722)

[7.2.4. Hướng dẫn tiêu chuẩn cho các kiểm soát 39](#_Toc122943723)

[7.2.5. Hướng dẫn tiêu chuẩn cho các hoạt động vòng đời 39](#_Toc122943724)

[7.3. Hướng dẫn ở mức hệ sinh thái 39](#_Toc122943725)

[7.3.1. Khái quát chung 39](#_Toc122943726)

[7.3.2. Hướng dẫn chuỗi xử lý dữ liệu 40](#_Toc122943727)

[7.3.3. Hướng dẫn quản lý rủi ro 41](#_Toc122943728)

[7.3.4. Hướng dẫn các hoạt động vòng đời 42](#_Toc122943729)

[8. Các thành phần chức năng bảo mật và quyền riêng tư 43](#_Toc122943730)

[8.1. Tổng quan 43](#_Toc122943731)

[8.2. Các thành phần chức năng cho cả bảo mật và quyền riêng tư 44](#_Toc122943732)

[8.3. Các thành phần chức năng cho quyền riêng tư 45](#_Toc122943733)

[8.4. Các chức năng đa lớp cho bảo mật và quyền riêng tư 47](#_Toc122943734)

[Phụ lục A](#_Toc122943735) [(Tham khảo)](#_Toc122943736) [Các ví dụ về các loại mối đe doạ bảo mật và quyền riêng tư 48](#_Toc122943737)

[Phụ lục B](#_Toc122943738) [(Tham khảo)](#_Toc122943739) [Các ví dụ về các loại kiểm soát bảo mật và quyền riêng tư 50](#_Toc122943740)

[Phụ lục C](#_Toc122943741) [(Tham khảo)](#_Toc122943742) [Các ví dụ về hệ sinh thái và kết quả điều phối các hoạt động bảo mật và quyền riêng tư 53](#_Toc122943743)

[Phụ lục D](#_Toc122943744) [(Tham khảo)](#_Toc122943745) [Ví dụ về kiểm soát bảo mật và quyền riêng tư cho mỗi vai trò BDRA 61](#_Toc122943746)

[Thư mục tài liệu tham khảo 69](#_Toc122943747)

|  |
| --- |
| **Lời nói đầu**TCVN ISO/IEC 20547-4:2022 hoàn toàn tương đương với ISO/IEC 20547-4:2020.TCVN ISO/IEC 20547-4:2022 do Viện Khoa học Kỹ thuật Bưu Điện biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố. |

|  |  |
| --- | --- |
| **T I Ê U C H U Ẩ N Q U Ố C G I A** | **TCVN ISO/IEC 20547-4:2022** |

**Công nghệ thông tin – Kiến trúc tham chiếu dữ liệu lớn – Phần 4: Bảo mật và quyền riêng tư**

*Information technology - Big data reference architecture - Part 4: Security and privacy*

# Phạm vi áp dụng

Tiêu chuẩn này đưa ra các yêu cầu bảo mật và quyền riêng tư cho kiến trúc dữ liệu lớn (BDRA) bao gồm các vai trò, các hoạt động, các thành phần chức năng dữ liệu lớn, đồng thời cung cấp các hướng dẫn về các hoạt động bảo mật và quyền riêng tư đối với dữ liệu lớn.

# Tài liệu viện dẫn

Tài liệu viện dẫn sau đây là cần thiết để áp dụng tiêu chuẩn này. Đối với tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất (bao gồm cả các sửa đổi, bổ sung).

TCVN 13238:2020 (ISO/IEC 20546), Công nghệ thông tin - Dữ liệu lớn - Tổng quan và từ vựng.

TCVN ISO/IEC 20547-3:2022 (ISO/IEC 20547-3:2020), Công nghệ thông tin - Kiến trúc tham chiếu dữ liệu lớn - Phần 3: Kiến trúc tham chiếu.

ISO/IEC/IEEE 15288, Systems and software engineering — System life cycle processes.

# Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa nêu trong TCVN 13238:2020 (ISO/IEC 20546).

# Chữ viết tắt

Theo mục đích của tiêu chuẩn này, các chữ viết tắt sau đây được áp dụng:

|  |  |  |
| --- | --- | --- |
| APT | advanced persistent threat | Tấn công có chủ đích |
| BRDA | big data reference architecture | Kiến trúc tham chiếu dữ liệu lớn |
| BD-S&P | big data security and privacy | Bảo mật và quyền riêng tư dữ liệu lớn |
| DDoS | Distributed Denial Of Service | Tấn công từ chối dịch vụ phân tán |
| LINDDUN | linkability, identifiability, non-repudiation, detectability, disclosure of information, una- wareness, non-compliance | Liên kết, nhận dạng, không từ chối, phát hiện, tiết lộ thông tin, không nhận thức, không tuân thủ  |
| PII | Personally Identifiable Information | Thông tin định dạng cá nhân |
| STRIDE | spoofing of user identity, tampering, repudiation, information disclosure, denial of ser- vice, elevation of privilege | Tấn công giả mạo danh tích người dùng, giả mạo, từ chối, tiết lộ thông tin, từ chối dịch vụ, leo thang đặc quyền |

# Tổng quan

## Các mối quan tâm về tính bảo mật và quyền riêng tư dữ liệu lớn

Mục phụ này giải quyết ba loại mối quan tâm:

* những rủi ro gây ra do các đặc tính của dữ liệu lớn;
* những thách thức bảo mật và quyền riêng tư từ dữ liệu lớn;
* khả năng điều phối hệ sinh thái cần thiết trong bối cảnh dữ liệu lớn.

Dữ liệu lớn có các đặc điểm chính về dung lượng, tốc độ chuyển đổi, tính đa dạng và tính biến đổi, và các đặc điểm chính của xử lý dữ liệu như tính thăng hoa, tinh chân thực và giá trị. Các đặc điểm này bao gồm thêm các rủi ro và cũng là các thách thức về khía cạnh bảo mật và quyền riêng tư của dữ liệu lớn.

* Dung lượng dữ liệu lớn có rủi ro liên quan đến lượng lớn dữ liệu ở các lớp khác nhau. Ví dụ, kho lưu trữ phân tán, nhiều tầng và truyền dẫn trên nhiều mạng với nhiều giao thức khác nhau.
* Tốc độ chuyển đổi dữ liệu có nguy cơ liên quan đến luồng chảy nhanh, tại đó dữ liệu được tạo ra, lưu trữ, phân tích và trực quan hóa. Kiểm soát bảo mật là một vấn đề đối với tốc độ chuyển đổi và dễ dàng bị bỏ qua.
* Tính đa dạng dữ liệu mang đến sự phức tạp hơn từ nhiều nguồn khác nhau dưới sự kiểm soát của tác nhân khác nhau. Sự phức tạp tất yếu dẫn đến các lỗ hổng. Một vấn đề do mang đến sự đa dạng dữ liệu lớn là khả năng suy luận danh tính từ một tập dữ liệu ẩn danh bằng cách tương quan với các cơ sở dữ liệu công khai và hoàn toàn vô hại.
* Tính biến đổi của dữ liệu có các rủi ro liên quan đến các thay đổi nhanh hơn về tốc độ dữ liệu, định dạnh/cấu trúc, các ngữ nghĩa và/hoặc chất lượng. Việc áp dụng các biện pháp kiểm soát bảo mật đối với bảo mật và quyền riêng tư dữ liệu có thể trở nên khó khăn hơn.
* Tính thăng hoa của dữ liệu có thể làm cho việc lưu vết kiểm tra và quản lý bảo mật trở nên khó khăn.
* Tính chân thực của dữ liệu mang đến các yêu cầu cao hơn đối với tính toàn vẹn, nhất quán và chính xác. Các rủi ro liên quan có thể được tổng hợp lại và phóng đại lên.
* Giá trị của dữ liệu cũng mang đến nhiều hơn các cuộc tấn công nhằm nhiều mục đích và lợi ích khác nhau.

Sự bùng nổ ứng dụng dữ liệu lớn mang đến các vấn đề nghiêm trọng hơn về bảo mật và quyền riêng tư đối với dữ liệu, ví dụ như các sự cố thường xuyên về vấn đề mất dữ liệu hoặc rò rỉ dữ liệu cá nhân, các giao dịch dữ liệu ngầm bất hợp pháp, gây ra việc lạm dụng dữ liệu và lừa đảo trên mạng, và làm nguy hiểm cho sự ổn định của xã hội và an ninh của quốc gia.

Dưới góc độ nền tảng công nghệ, do sự xuất hiện liên tục của nhiều loại công nghệ dữ liệu lớn, kiến trúc kỹ thuật mới, các nền tảng hỗ trợ và phần mềm dữ liệu lớn, các khả năng bảo mật và quyền riêng tư sau đây là cần thiết trong bối cảnh dữ liệu lớn.

* Các biện pháp kiểm soát bảo mật truyền thống trong bối cảnh dữ liệu lớn là cần thiết.

Các đặc điểm như là đồ sộ, đa nguồn, không đồng nhất, động và các đặc điểm khác của dữ liệu lớn dẫn tới sự khác biệt về bảo mật ứng dụng dữ liệu so với một môi trường đóng. Các ứng dụng dữ liệu lớn thường sử dụng kiến trúc lưu trữ và tính toán phân tán mở với các hỗ trợ cơ sở phức tạp nhằm cung cấp kho lưu trữ phân tán dữ liệu lớn và các dịch vụ tính toán hiệu suất cao. Các công nghệ và kiến trúc mới này khiến ranh giới mạng của các ứng dụng dữ liệu lớn trở nên mờ nhạt, do đó các biện pháp bảo mật dựa trên ranh giới truyền thống không còn hiệu lực. Trong khi đó tấn công có chủ đích (APT), tấn công từ chối dịch vụ phân tán (DDoS), khai thác dữ liệu dựa trên máy học, khám phá quyền riêng tư và các loại tấn công khác khiến cho các biện pháp phòng thủ, phát hiện và các biện pháp kiểm soát bảo mật truyền thống khác lộ ra các khiếm khuyết nghiêm trọng. Ví dụ, đối với việc cung cấp quản lý dữ liệu an toàn và thông tin tình báo mối đe dọa, cung cấp kho lưu trữ dữ liệu an toàn cho dữ liệu lớn cũng như việc tạo, truyền, lưu trữ, phân tích và loại bỏ dữ liệu nhật ký an toàn trở nên cực ký khó khăn. Ngoài ra, các phương pháp tiếp cận kỹ thuật đối với bảo vệ quyền riêng tư, học máy, cơ chế mã hóa đối với bảo mật lấy dữ liệu làm trung tâm và kiểm soát truy cập là cần thiết.

Để biết thêm thông tin các yêu cầu của bảo mật và quyền riêng tư dữ liệu lớn, hãy tham khảo các cân nhắc kỹ thuật bảo mật và quyền riêng tư trong các trường hợp sử dụng được cung cấp bởi TCVN 13239-2:2020.

* Bảo mật và quyền riêng tư cần được cung cấp cho cơ sở hạ tầng tính toán phân tán và lưu trữ dữ liệu của dữ liệu lớn.

Vấn đề này đòi hỏi tính toán phân tán và sự phổ biến thông tin phải an toàn và bảo vệ quyển riêng tư. Dữ liệu lớn cần các giải pháp có thể mở rộng và phân tán cho các kho dữ liệu an toàn cũng như để kiểm tra và điều tra nguồn gốc dữ liệu. Tính toàn vẹn dữ liệu đối với việc truyền luồng dữ liệu từ các cảm biến khác nhau và các điểm cuối khác cần phải được cung cấp. Phân tích thời gian thực đối với thông tin tình báo các mối đe dọa cần xử lý một lượng lớn thông tin liên quan đến vấn đề bảo mật như là luồng lưu lượng và thông tin nhật ký.

* Cơ chế bảo mật nền tảng cần phải được cải thiện trong bối cảnh bảo mật và quyền riêng tư dữ liệu lớn.

Nhìn chung, các ứng dụng dữ liệu hiện có sử dụng nền tảng và công nghệ quản lý dữ liệu lớn như là Hadoop HBase/Hive, Cassandra/Spark, MongoDB. Khi bắt đầu thiết kế, các nền tảng và công nghệ này chủ yếu được coi như là sử dụng trong một mạng nội bộ đáng tin cậy, ít được xem xét về vấn đề xác thực, phân quyền, các dịch vụ khóa và đánh giá bảo mật. Mặc dù các phần mềm đã được cải thiện, như là bổ sung cơ chế xác thực Kerberos, nhưng khả năng bảo mật tổng thể vẫn còn khá yếu. Trong khi đó, các thành phần mã nguồn mở bên thứ ba thường xuyên được sử dụng trong các ứng dụng dữ liệu lớn. Do thiếu chứng nhận bảo mật và quản lý thử nghiệm nghiêm ngặt đối với các thành phần này, khả năng phòng ngừa các lỗ hổng phần mềm cũng như các cửa hậu độc hại ở trong các ứng dụng dữ liệu lớn là không đủ.

* Khả năng kiểm soát truy cập ứng dụng trong bối cảnh dữ liệu lớn là cần thiết.

Bởi vì sự đa dạng các loại dữ liệu và phạm vi rộng rãi các ứng dụng của dữ liệu lớn, Việc này thường được sử dụng để cung cấp nhiều dịch vụ cho các người dùng có danh tính và mục đích khác nhau từ các tổ chức hoặc bộ phận khác nhau. Nói chung, kiểm soát truy cập là một cách hiệu quả để có thể đạt được truy cập có kiểm soát vào dữ liệu. Tuy nhiên, do có một lượng lớn các người dùng dữ liệu không xác định và dữ liệu được truy cập, việc thiết lập trước các vai trò và các quyền truy cập dữ liệu là rất khó khăn. Mặc dù quyền người dùng truy cập dữ liệu có thể được phân loại trước nhưng do có một lượng lớn các vai trò, rất khó để định nghĩa kiểm soát các quyền của từng vai trò. Vì vậy, việc xác định chính xác các phạm vi dữ liệu mà mỗi người dùng được truy cập mà không phải triển khai thêm môt mô hình kiểm soát truy cập mới hơn như kiểm soát truy cập cơ sở (ABAC) là rất khó. Điều này cũng gây ra vấn đề đối với nguyên tắc tối thiểu hóa dữ liệu trong ISO/IEC 29100.

* Các cơ chế bảo mật và quyền riêng tư có thể mở rộng là cần thiết.

Khi thiết kế và áp dụng các cơ chế bảo mật và quyền riêng tư như là quản lý khóa, quản lý truy cập và định danh, khử nhận dạng,v.v, trong môi trường dữ liệu lớn thì không chỉ các chức năng bảo mật và quyền riêng tư cần được xem xét, khả năng mở rộng của các cơ chế này cũng cần được tính đến để hỗ trợ việc xử lý dữ liệu có dung lượng lớn và tốc độ chuyển đổi cao.

Từ góc độ ứng dụng dữ liệu, do các đăc điểm Vs lớn (dung lượng, tính đa dạng, tốc độ chuyển đổi và tính biến đổi) của dữ liệu lớn và giá trị khổng lồ trong dữ liệu lớn, các khả năng bảo mật và quyền riêng tư sau đây là cần thiết trong bối cảnh dữ liệu lớn:

* Khả năng bảo vệ dữ liệu trong bối cảnh dữ liệu lớn là cần thiết.

Trong xã hội mạng mở rộng, dung lượng dữ liệu lớn khổng lồ với giá trị tiềm năng không thể đo được làm cho vấn đề này trở nên được ưa chuộng và dễ dàng trở thành một mục tiêu tấn công mạng đáng kể. Trong những năm gần đây, các sự cố bảo mật thông tin thường xuyên xảy ra, ví dụ như là rò rỉ tài khoản mail cá nhân, thông tin an sinh xã hội và số tài khoản ngân hàng. Việc triển khai các hệ thống phân tán, môi trường mạng mở, ứng dụng dữ liệu phức tạp và lượng lớn người dùng truy cập, tất cả đều khiến dữ liệu lớn đối mặt với các thách thức lớn hơn về tính bí mật, tính toàn vẹn, tính khả dụng,...

* Khả năng bảo vệ dữ liệu cá nhân trong bối cảnh dữ liệu lớn là cần thiết.

Do có một lượng lớn dữ liệu cá nhân trong các hệ thống dữ liệu lớn, khi một sự cố bảo mật xảy ra như là lạm dụng dữ liệu, đánh cắp nội bộ hoặc tấn công mạng, thì hậu quả của việc rò rỉ dữ liệu cá nhân còn nghiêm trọng hơn so với các hệ thống thông tin thông thường. Mặt khác, lợi thế của việc tạo ra giá trị thông qua phân tích và sử dụng lượng lớn dữ liệu có thể bị tổn hại do nguy cơ rò rỉ dữ liệu cá nhân trong quá trình phân tích toàn diện dữ liệu đa nguồn tại nơi mà các nhà phân tích có thể dễ dàng khám phá dữ liệu cá nhân thông qua phân tích tương quan.

* Khả năng xác thực dữ liệu trong bối cảnh dữ liệu lớn là cần thiết.

Dữ liệu trong các hệ thống dữ liệu lớn có thể từ nhiều nguồn khác nhau như các loại cảm biến, hành động tải lên và các trang web công khai. Ngoài các nguồn dữ liệu đáng tin cậy, có một lượng lớn các nguồn dữ liệu không đáng tin cậy. Nhiều kẻ tấn công thậm chí cố tình làm sai lệch dữ liệu nhằm mục đích thu gây ảnh hưởng đến kết quả phân tích dữ liệu. Do đó, việc xác minh tính xác thực và nguồn gốc của dữ liệu là rất quan trọng. Tuy nhiên, có rất nhiều khó khăn trong việc xác minh tính xác thực toàn bộ dữ liệu bởi vì hiệu suất hạn chế của các thiết bị thu thập thông tin đầu cuối, sự thiếu sót công nghệ, lượng thông tin hạn chế và sự đa dạng cũng như phức tạp của các nguồn.

* Khả năng bảo vệ quyền của chủ sơ hữu dữ liệu trong bối cảnh dữ liệu lớn là cần thiết.

Trong quá trình ứng dụng dữ liệu lớn, dữ liệu có thể được truy cập bởi nhiều người khác nhau, chuyển từ nhà kiểm soát này sang nhà kiểm soát khác và thậm chí bị khai thác để tạo ra dữ liệu mới. Do đó, trong quá trình trao đổi và chia sẻ dữ liệu, có trường hợp quyền sở hữu dữ liệu của chủ sở hữu và quyền sử dụng dữ liệu của nhà quản lý dữ liệu bị tách biệt, điều đó ám chỉ rằng dữ liệu có thể nằm ngoài tầm kiểm soát của chủ sở hữu và mang tới các rủi ro như là lạm dụng dữ liệu, quyền sở hữu dữ liệu mập mờ, không rõ trách nhiệm giám sát bảo mật dữ liệu, xâm hại tới quyền và lợi ích của các chủ sở hữu dữ liệu.

Dữ liệu lớn liên quan đến hệ sinh thái, hoặc mạng lưới của các tổ chức cộng tác để thu thập, phân tích và chia sẻ dữ liệu. Những sự hợp tác sau đây là cần thiết trong bối cảnh dữ liệu lớn:

* Cộng tác giữa các bên liên quan để đảm bảo các yêu cầu về bảo mật và quyền riêng tư tổng thể của hệ sinh thái cũng như các yêu cầu về bảo mật và quyền riêng tư của các cá nhân tổ chức là nhất quán;
* Cộng tác giữa các bên liên quan để đảm bảo việc quản lý rủi ro tổng thể hệ sinh thái cũng như quản lý rủi ro cá nhân tổ chức là nhất quán; và
* Cộng tác giữa các bên liên quan để đảm bảo rằng các cá nhân tổ chức đảm bảo việc xử lý nhất quán các tài sản cần được bảo vệ.

## Mục tiêu bảo mật và quyền riêng tư

Các ứng dụng dữ liệu lớn có các mục tiêu về bảo mật và quyền riêng tư. Bảng 1 mô tả ví dụ các mục tiêu bảo mật. Bảng 2 mô tả ví dụ các mục tiêu quyền riêng tư. Chú ý rằng Bảng 2 mô tả các cách thay thế để xem xét các mục tiêu.

Bảng 1 - Các mục tiêu bảo mật

|  |  |  |
| --- | --- | --- |
| **Mục tiêu** | **Mô tả** | **Ví dụ** |
| Mục đích bảo mật[TừISO/IEC 270001] | Tính bí mật | Đảm bảo thông tin không được cung cấp hoặc tiết lộ cho các cá nhân, thực thể, quy trình không có thẩm quyền | Đường truyền dữ liệu thu thập được bảo vệ, truy cập được bảo vệ với các hệ thống xác thực phù hợp, xử lý dữ liệu được bảo vệ và kho lưu trữ được bảo vệ. |
| Tính toàn vẹn | Đảm bảo tính chính xác và đầy đủ của dữ liệu trong suốt vòng đời của dữ liệu | Bảo vệ tính toàn vẹn trong suốt quá trình truyền tải, xử lý dữ liệu, cũng như ở cấp độ lưu trữ bằng cách sử dụng các hệ thống như là chữ ký điện tử. |
| Tính khả dụng | Đảm bảo khả năng tiếp cận và sử dụng theo yêu cầu của một thực thể được ủy quyền | Ngăn chặn sự gián đoạn dịch vụ bởi sự cố mất điện, hỏng hóc phần cứng, hoặc tấn công từ chối dịch vụ bằng các hệ thống như là hệ thống dự phòng. |

Bảng 2 - Các mục tiêu quyền riêng tư

| **Mục tiêu**  | **Mô tả** |
| --- | --- |
| Các nguyên tắc quyền riêng tư [TừISO/IEC TR 27550] | Sự đồng thuận và sự lựa chọn | Cung cấp các chủ PII các cơ chế rõ ràng, nổi bật, dễ hiểu, dễ tiếp cận và giá cả phải chăng để thực hiện sự lựa chọn và đưa ra sự đồng thuận liên quan đến việc xử lý PII tại thời điểm thu thập.  |
| Tính chính đáng của mục đích và đặc điểm kỹ thuật | Giả định rằng các mục đích sử dụng tuân thủ với các luật hiện hành và dựa trên cơ sở pháp lý cho phép. |
| Hạn chế thu thập | Hạn chế việc thu thập PII trong phạm vi giới hạn của luật hiện hành và khi thực sự cần thiết cho một mục đích cụ thể |
| Giảm thiểu dữ liệu | Giảm thiểu việc xử lý PII |
| Hạn chế duy trì sử dụng và tiết lộ | Hạn chế việc sử dụng, duy trì và tiết lộ (bao gồm cả chuyển giao) PII chỉ cho những việc cần thiết để thực hiện các mục đích cụ thể, rõ ràng và hợp pháp. |
| Chính xác và chất lượng | Đảm bảo rằng PII được xử lý là chính xác, hoàn thiện, cập nhật (trừ khi có cơ sở pháp lý để lưu trữ các dữ liệu lỗi thời), đầy đủ và phù hợp để sử dụng. |
| Công khai, minh bạch và thông báo | Cung cấp các chủ PII thông tin rõ ràng và dễ tiếp cận về các chính sách điều khiển, thủ tục và thông lệ liên quan đến xử lý PII của nhà điều khiển PII. |
| Tham gia và truy cập cá nhân | Cung cấp các chủ PII khả năng truy cập và kiểm tra PII của họ miễn là danh tính của họ được xác thực với mức độ đảm bảo thích hợp và truy cập đó không bị ngăn cấm bởi pháp luật. |
| Trách nhiệm giải trình | Việc xử lý PII đòi hỏi nghĩa vụ chăm sóc và áp dụng các biện pháp cụ thể và thiết thực để bảo vệ nó. |
| Bảo mật thông tin | Bảo vệ PII theo thẩm quyền với các biện pháp kiểm soát ở mức hoạt động, chức năng và chiến lược để đảm bảo tính toàn vẹn, bí mật và sẵn sàng của PII và bảo vệ khỏi các rủi ro như là truy cập trái phép, phá hủy, sử dụng, thay đổi, tiết lộ hoặc mất mát trong toàn bộ vòng đời của nó. |
| Tuân thủ quyền riêng tư | Xác minh và chứng minh rằng quá trình đáp ứng các yêu cầu bảo vệ dữ liệu và quyền riêng tư bằng cách thực hiện đánh giá nội bộ định kỳ hoặc thông qua bên thứ ba đáng tin cậy. |
| Các mục đích quyền riêng tư[TừISO/IEC TR 27550] | Tính không liên kết | Đảm bảo rằng một chủ PII có thể sử dụng nhiều tài nguyên hoặc dịch vụ mà ngươi khác không thể liên kết chúng lại với nhau.VÍ DỤ: Một người dùng sử dụng hai tài khoản khác nhau cho một dịch vụ liên quan đến phân tích dữ liệu lớn. |
| Tính minh bạch | Đảm bảo được một mức độ rõ ràng phù hợp đối với các quy trình xử dữ liệu liên quan đến quyền riêng tư để quá trình thu thập, xử lý và sử dụng thông tin có thể hiểu được và xây dựng lại bất cứ khi nào.VÍ DỤ: Tài liệu dễ hiểu bao gồm công nghệ, tổ chức và trách nhiệm mà chủ PII có thể tiếp cận được |
| Tính giao thoa | Đảm bảo rằng các chủ PII, nhà điều khiển PII, nhà xứ lý PII và các cơ quan giám sát có thể can thiệp vào toàn bộ quá trình xử lí dữ liệu liên quan đến quyền riêng tư.VÍ DỤ: Các quá trình gây ảnh hưởng hoặc ngưng trệ quy trình xử lý dữ liệu hoàn toàn hoặc một phần, đảo ngược quyết định tự động hoặc thủ công, các biện pháp phòng ngừa khả năng di chuyển dữ liệu |
| Mục tiêu kỹ thuật quyền riêng tư[TừISO IEC TR 27550] | Khả năng dự đoán | Cung cấp sự hiểu biết đáng tin cậy về những gì đang xảy ra trong quy trình xử lý PII trong hệ thống.VÍ DỤ: Phát triển khả năng xử lý PII có thể lặp lại. Liên quan đến mục tiêu bảo vệ tính minh bạch. |
| Khả năng quản lý | Quản trị PII với đủ độ chi tiết để có thế áp dụng các mức kiểm soát phù hợp.VÍ DỤ: Phát triển quản lý ưu tiên quyền riêng tư để cho phép chủ PII một mức độ kiểm soát phù hợp. Liên quan đến mục tiêu bảo vệ khả năng can thiệp. |
| Tính không liên quan | Tích cực bảo vệ hoặc “làm mờ” danh tính của một cá nhân hoặc các hoạt động có liên quan khỏi sự phơi bày không cần thiết trong các quá trình giao dịch.VÍ DỤ: Phát triển khả năng xử lý dữ liệu sức khỏe ẩn danh. Liên quan đến mục tiêu bảo vệ tính không liên kết. |

Khoản 6 đến 8 nằm trong bối cảnh các hệ thống dữ liệu lớn có các mối quan tâm và mục tiêu về bảo mật và quyền riêng tư (S&P) như trên.

Bảo mật và quyền riêng tư dữ liệu lớn (BD-S&P) sẽ dựa trên kiến trúc tham chiếu dữ liệu (BDRA) được định nghĩa trong TCVN ISO/IEC 20547-3:2022.

# Khía cạnh bảo mật và quyền riêng tư của BRDA góc nhìn người dùng

## Hoạt động quản trị

### Mục đích

Quản trị dữ liệu được định nghĩa trong TCVN ISO/IEC 20547-3:2022 là việc quản trị của một tổ chức và chú trọng vào khía cạnh dữ liệu của tổ chức. Mục đích của cát hoạt động quản trị BD-S&P là thiết lập và duy trì sự nhất quán và liên kết của BD-S&P với các mục tiêu và ràng buộc liên quan đến các nhu cầu bảo mật và quyền riêng tư của một tổ chức và các bên liên quan hay các nhóm quan tâm của tổ chức đó.

CHÚ THÍCH: Việc quản trị BD-S&P cũng có thể áp dụng trong nội bộ tổ chức, hoặc cho một hệ sinh thái. Ví dụ, một tổ chức phụ trách một thị trường dữ liệu lớn có thể cung cấp các chính sách quản trị cho các bên tham gia.

### Chuẩn bị và lập kế hoạch cho nỗ lực quản trị BD S&P

1. Thiết lập chiến lược BD-S&P xuất phát từ các mục tiêu, chiến lược và tầm nhìn tổ chức.
2. Thiết lập vai trò, trách nhiệm, trách nhiệm giải trình, quyền hạn và cơ cấu tổ chức nhằm hỗ trợ nỗ lực quản trị BD-S&P và báo cáo các yêu cầu.
3. Thiết lập cơ cấu tổ chức quản trị BD S&P phù hợp với các vai trò, quyền hạn, trách nhiệm và trách nhiệm giải trình được thiết lập.
4. Thiết lập các nguyên tắc chỉ đạo và hướng dẫn công việc để thực thi BD-S&P.

CHÚ THÍCH: Các hướng dẫn công việc mô tả các bước cần thực hiện bởi những người thực hiện các hoạt động quản trị. Điều này để đảm bảo các quyết định của quy trình là minh bạch và tuân thủ một cách nhất quán. Đôi khi, một ban thư ký được sử dụng để quản lý các hướng dẫn công việc này và để đảm bảo rằng chúng được tuân thủ theo đúng cách.

1. Thiết lập các diễn đàn về quyết định để thực hiện các hướng dẫn công việc quản trị BD-S&P.
2. Định nghĩa các thủ tục để xác định, quản lý, kiểm tra và phổ biến thông tin liên quan đến các quyết định về quản trị BD-S&P.
3. Liên kết các thủ tục với chiến lược BD-S&P.
4. Ánh xạ các thủ tục tới các nguồn lực và ràng buộc để hỗ trợ chiến lược, lập kế hoạch và ra quyết định.
5. Lập kế hoạch cho nỗ lực quản trị BD-S&P.
6. Thiết lập phạm vi cho nỗ lực quản trị BD-S&P.
7. Thiết lập các thước đo cho nỗ lực quản trị BD-S&P.
8. Xác định các thông tin và dữ liệu cần thiết cho nỗ lực quản trị BD-S&P.
9. Xác định và định nghĩa các yếu tố công việc quản trị BD-S&P và các nguồn lực liên quan.
10. Xây dựng lịch trình quản trị BD-S&P và định nghĩa các cột mốc có liên quan.
11. Có được các phê duyệt và kinh phí cần thiết cho kế hoạch.
12. Thu thập thông tin và dữ liệu cần thiết cho nỗ lực quản trị BD-S&P.

### Giám sát, đánh giá và kiểm soát các hoạt động quản trị BD-S&P

1. Giám sát và đánh giá các chỉ số cho nỗ lực quản trị BD-S&P.
2. Xác định và đánh giá các rủi ro và cơ hội liên quan đến nỗ lực quản trị BD-S&P.
3. Đảm bảo các quy trình khác đang sử dụng đúng các chỉ thị và hướng dẫn quản trị BD-S&P.
4. Báo cáo các kế hoạch và tình trạng hoạt động quản trị BD-S&P phù hợp với các yêu cầu báo cáo.
5. Đánh giá và kiểm soát nỗ lực quản trị BD-S&P.
6. Quản lý rủi ro liên quan đến quản trị BD-S&P.

### Thiết lập các mục tiêu quản trị BD-S&P

1. Kiểm tra các nhu cầu nghiệp vụ liên quan đến dữ liệu lớn hiện tại và tương lai đã biết.
2. Kiểm tra các mục tiêu doanh nghiệp liên quan đến dữ liệu lớn hiện tại và tương lai cần đạt được, như là duy trì lợi thế cạnh tranh.
3. Kiểm tra và đưa ra đánh giá về tầm nhìn doanh nghiệp liên quan đến dữ liệu lớn hiện tại và tương lai, bao gồm các chiến lược, các đề xuất và sắp xếp cung ứng (cho dù là bên trong, bên ngoài, hoặc cả hai) để hỗ trợ các mục tiêu doanh nghiệp liên quan đến dữ liệu lớn.

CHÚ THÍCH 1: Việc kiểm tra có thể xem xét các áp lực bên trong hoặc bên ngoài tác động lên doanh nghiệp, như là thay đổi nghiệp vụ, thay đổi công nghệ, xu hướng kinh tế xã hội và ảnh hưởng chính trị.

1. Kiểm tra các mục tiêu BD-S&P của các chiến lược và đề xuất đang được đánh giá.
2. Kiểm tra các nhu cầu liên quan đến dữ liệu lớn hiện tại và tương lai cho các nhiệm vụ được doanh nghiệp hỗ trợ.
3. Kiểm tra các mục tiêu nhiệm vụ liên quan đến dữ liệu lớn hiện tại và tương lai cần phải đạt được.
4. Kiểm tra và đánh giá khả năng sử dụng dữ liệu lớn trong tương lại, bao gồm các chiến lược, đề xuất và sắp xếp cung ứng (bên trong, bên ngoài hoặc cả hai) trong hỗ trợ các mục tiêu nhiệm vụ.

CHÚ THÍCH 2: Việc kiểm tra có thể xem xét các áp lực bên trong hoặc bên ngoài tác động lên doanh nghiệp, như là thay đổi công nghệ, xu hướng kinh tế xã hội và ảnh hưởng chính trị.

1. Kiểm tra các mục tiệu BD-S&P của các chiến lược và đề xuất đang được đánh giá.
2. Thiết lập chiến lược BD-S&P bằng việc đưa ra các quyết định liên quan đến quản trị BD-S&P.
3. Khám phá, phát triển, định nghĩa và đánh giá tổng thể các mục tiêu BD-S&P nói chung.
4. Xác định công việc cần thực hiện để đạt được các mục tiêu này.
5. Tạo một cấu hình các nguồn lực là thành phần cần thiết để đáp ứng các mục tiêu này.
6. Thiết lập một phương tiện đo lường hiệu quả quản trị.
7. Định nghĩa các chính sách quản trị BD-S&P liên quan đến BD-S&P.
8. Định nghĩa bộ nguyên tắc quản trị áp dụng cho BD-S&P.
9. Xác định sự tuân thủ các mục tiêu dựa trên các tiêu chí và chiến lược tuân thủ quản trị.
10. Thiết lập các tiêu chí quản lý để kiểm soát các thông lệ, các cho phép và tuân thủ quản trị BD-S&P.
11. Xác định các mục tiêu BD-S&P cần theo đuổi và mức độ mong muốn đạt được cho mỗi mục tiêu.

### Chỉ đạo BD-S&P

1. Thiết lập và ban hành chỉ đạo quản trị dưới hình thức các chỉ thị và hướng dẫn cho BD-S&P.
2. Phát triển và ban hành (các) chỉ thị quản trị thúc đẩy sự phát triển thích hợp của BD-S&P.
3. Triển khai khuôn khổ quản trị hỗ trợ cho chỉ thị quản trị này để định nghĩa cấu trúc tổ chức và khái niệm cũng như cung cấp phương pháp ra quyết định có cấu trúc.
4. Thiết lập cơ chế ra quyết định nhằm giảm thiểu hoặc tránh những xung đột lợi ích có thể xảy ra với sự leo thang trong doanh nghiệp nếu như các vấn đề không được giải quyết hợp lý bởi quản trị BD-S&P.
5. Phân công trách nhiệm, chỉ đạo việc chuẩn bị và thực thi các chỉ thị, cho các tiêu chuẩn và chính sách định hướng cho các nỗ lực BD-S&P.
6. Đưa ra quyết định chiến lược trong phạm vị trách nhiệm và quyền hạn quản trị BD-S&P.
7. Xem xét và truyền đạt các quyết định.

### Theo dõi và đánh giá sự tuân thủ với các chỉ thị và hướng dẫn quản trị BD-S&P

1. Giám sát việc quản trị BD-S&P của doanh nghiệp bằng cách sử dụng các phương tiện thích hợp.

CHÚ THÍCH 1: Không giám sát BD-S&P. Để xem việc BD-S&P đang giúp đạt được các mục đích và mục tiêu doanh nghiệp tốt tới đâu, quản trị BD-S&P có thể giám sát các chỉ số đo lường từ việc phát triển và sử dụng các thực thể thực tế dựa trển BD-S&P.

1. Thiết lập phương tiện để giám sát việc tuân thủ với các chỉ thị và hướng dẫn quản trị BD-S&P.

CHÚ THÍCH 2: Bảng điều khiển là một cách thông dụng để thực hiện việc này.

1. Giả định trước rằng BD-S&P tuân thủ các nghĩa vụ bên ngoài (điều tiết, lập pháp, luật pháp, hợp đồng) và thực tiễn công việc nội bộ.
2. Khi thích hợp, cơ quan quản trị BD-S&P có thể truy cập trực tiếp vào một thực thể được xây dựng theo thiết kế BD-S&P dưới sự bảo trợ của cơ quan quản trị.

CHÚ THÍCH 3: Quyền truy cập này của ban quản trị nhằm cho phép xác minh rằng một thệ thống, một doanh nghiệp, một hạng mục phần mềm, một dịch vụ hoặc các loại thực thể BD-S&P khác tuân thủ các nghĩa vụ được thiết lập bởi các chỉ thị quản trị. Việc chỉ kiểm tra sự phù hợp BD-S&P có thể là không đủ vì các đặc trưng có thể thiếu các bản dịch thích hợp sang thiết kế hoặc hoạt động của thực thể.

1. Thiết lập một ma trận trách nhiệm để đảm bảo các trách nhiệm được phân công là phù hợp.
2. Theo dõi các kế hoạch và trạng thái quản lý và đánh giá sự tuân thủ các chỉ trị và hướng dẫn quản trị cho BD-S&P.
3. Kiểm tra tính hiệu quả của các chính sách quản trị BD-S&P và bắt đầu các bước sửa đổi các chính sách khi cần thiết.
4. Thu thập các bài học kinh nghiệm liên quan đến quản trị BD-S&P được báo cáo từ các cam kết trước đó và cung cấp các bài học này cho các dự án tương lai.

### Rà soát thực hiện các hướng dẫn và chỉ thị quản trị BD-S&P và chuẩn bị cho thay đổi

CHÚ THÍCH: Hoạt động này bao gồm các nhiệm vụ cần thiết để cơ quan quản trị BD-S&P hoàn thiện nỗ lực quản trị BD-S&P.

1. Rà soát các thông tin để khẳng định công việc quản trị BD-S&P đã hoàn thành và các mục tiêu BD-S&P đã đạt được.
2. Giả định rằng các tuân thủ đối với các nghĩa vụ và tiêu chuẩn hiện hành có ảnh hưởng đến việc quản trị BD-S&P.
3. Thiết lập các thủ tục để điều tra và thu thập các lí do khác nhau dẫn đến việc không thực hiện các chỉ thị và hướng dẫn quản trị.
4. Lưu lại các bài học kinh nghiệm và truyền đạt cho các bên liên quan.
5. Đóng góp các thông lệ tốt nhất cho quản trị BD-S&P.
6. Xem xét kỹ lưỡng tính hiệu quả của các chỉ thị và hướng dẫn BD-S&P.
7. Xác định và lựa chọn các thay đổi cần thực hiện đối với các chỉ thị và hướng dẫn BD-S&P.
8. Kết hợp các thay đổi vào các chỉ thị và hướng dẫn quản trị BD-S&P.

## Các hoạt động quản lý

### Mục đích

Mục đích các hoạt động quản lý BD-S&P là để đảm bảo việc thực hiện đúng các chỉ thị quản trị BD-S&P và đạt được các mục tiêu BD-S&P một cách hiệu quả và kịp thời.

### Chuẩn bị và lên kế hoạch cho nỗ lực quản trị BD-S&P

1. Xác định phương pháp tiếp cận, ràng buộc, phương pháp, công cụ và kỹ thuật quản lý BD-S&P dựa trên các chính sách, chỉ thị và hướng dẫn quản trị BD-S&P.

CHÚ THÍCH: Quản lý theo các mục tiêu, quản lý bằng đo lường và quản lý băng các chính sách là các ví dụ về phương pháp tiếp cận quản lý.

1. Xây dựng điều lệ quản lý BD-S&P.
2. Xác định các tài sản của tổ chức (con người, nguồn lực, quy trình) ảnh hưởng đến việc quản lý BD-S&P.
3. Xác định các tài sản tri thức (thông tin lịch sử, các vấn đề và giải pháp khiếm khuyết, kết quả thành công) có thể hỗ trợ trong việc quản lý BD-S&P
4. Xác định các yếu tố và tiêu chí bên trong và bên ngoài ảnh hưởng đến việc quản lý BD-S&P.
5. Xác định các điểm trong và ngoài phạm vị ảnh hưởng đến việc quản lý BD-S&P.
6. Xây dựng bảng kê công việc phù hợp với điều lệ quản lý BD-S&P.
7. Định nghĩa các mục tiêu quản lý BD-S&P có thể đo lường được và các tiêu chí thành công có liên quan cho BD-S&P.
8. Xây dựng cơ cấu tổ chức quản lý BD-S&P.
9. Xác định các vai trò quản lý, trách nhiệm và quyền hạn cần thiết có liên quan hoặc tham gia vào quản lý BD-S&P.
10. Định nghĩa hệ thống phân cấp kiểm soát quản lý BD-S&P tương ứng với các vai trò và trách nhiệm được xác định.
11. Đảm bảo phân quyền phù hợp trách nhiệm quản lý trong hệ thống phân cấp kiểm soát quản lý BD-S&P.
12. Đảm bảo phân bổ vai trò thích hợp cho những người đóng vai trò được xác định trong hệ thống phân cấp quản lý BD-S&P.
13. Lập kế hoạch cho nỗ lực quản lý BD-S&P
14. Thiết lập phạm vi nỗ lực quản lý BD-S&P.
15. Xác định các chỉ số cho nỗ lực quản lý BD-S&P.
16. Thu thập thông tin và dữ liệu cần thiết cho nỗ lực BD-S&P.
17. Có được quyền truy cập vào các bên hỗ trợ cần thiết cho nỗ lực quản lý BD-S&P.
18. Xác định và định nghĩa các yếu tố công việc quản lý BD-S&P và các nguồn lực liên quan.
19. Xây dựng lịch trình quản lý BD-S&P và định nghĩa các cột mốc liên quan.
20. Có được các phê duyệt cần thiết cho kế hoạch quản lý BD-S&P.
21. Đảm bảo rằng BD-S&P được thiết lập và duy trì phù hợp với các kế hoạch liên quan.

### Giám sát, đánh giá và kiểm soát các hoạt động quản lý kiến trúc

1. Báo cáo các kế hoạch và tình trạng hoạt động quản lý BD-S&P.
2. Giám sát và đánh giá việc tuân thủ các chỉ thị và hướng dẫn quản trị BD-S&P.
3. Giám sát và đánh giá các chỉ số cho nỗ lực quản lý BD-S&P.
4. Xác định và đánh giá các rủi ro và cơ hội liên quan đến nỗ lực quản lý BD-S&P.
5. Đảm bảo các quy trình khác (ví dụ: quy trình vòng đời doanh nghiệp, quy trình vòng đời hệ thống) đang sử dụng đúng các hướng dẫn công việc quản lý BD-S&P.
6. Báo cáo các kế hoạch và tình trạng hoạt động quản lý BD-S&P phù hợp với các yêu cầu báo cáo.
7. Đánh giá và kiểm soát nỗ lực quản lý BD-S&P.
8. Quản lý rủi ro liên quan đến quản lý BD-S&P.

### Xây dựng cách tiếp cận quản lý BD-S&P

1. Xây dựng các kế hoạch quản lý BD-S&P phù hợp với định hướng quản trị BD-S&P.
2. Xác định các yêu cầu BD-S&P và các mối quan tâm khác.
3. Định nghĩa bản mô tả phạm vi quản lý BD-S&P (mô tả phạm vi, tiêu chí chấp thuận, phân phối, loại trừ, ràng buộc, giả định).
4. Thiết lập các mục tiêu quản lý BD-S&P cụ thể nhằm giải quyết các mục tiêu BD-S&P và làm rõ lý do cho sự đầy đủ của chúng.
5. Ưu tiên các mục tiêu về tầm quan trọng trong việc đạt được các mục tiêu BD-S&P.
6. Tạo một định nghĩa công việc nhằm cung cấp một khung chung cho việc lập kế hoạch và kiểm soát tổng thể BD-S&P.
7. Vạch ra các nhiệm vụ (ví dụ như đường lối hoạt động) cần để đạt được các mục tiêu quản lý BD-S&P và sắp xếp các nhiệm vụ theo mức độ quan trọng để được các mục tiêu này.
8. Định nghĩa các nguồn lực tổ chức cần thiết để thực hiện các nhiệm vụ.
9. Thiết lập các phương pháp đánh giá sự tiến bộ của các nhiệm vụ đối với việc hoàn thành mục tiêu.
10. Xác định các đường lối hoạt động thay thế (kế hoạch dự phòng) trong trường hợp không đạt được các mục tiêu nào đó.
11. Đảm bảo định nghĩa công việc nhất quán với các mục tiêu quản lý BD-S&P và bao gồm các mức độ không chắc chắn và thay đổi được dự đoán trước.
12. Thiết lập các nguồn lực cần thiết để thực hiện các yếu tố công việc quản lý BD-S&P và phân công trách nhiệm, quyền hạn cho hệ thống phân cấp quản lý.

Xây dựng định nghĩa nguồn lực cần thiết nhằm mang đến kết quả.

1. Định nghĩa các biện pháp quản lý cho phép đánh giá sự tuân thủ với các mục tiêu quản lý BD-S&P.

Định nghĩa các hệ thống đo lường có thể hỗ trợ cho việc đo lường các hoạt động BD-S&P.

1. Xây dựng lịch trình quản lý BD-S&P phù hợp với (các) kế hoạch quản lý BD-S&P.
2. Xây dựng ngân sách để tạo và quản lý BD-S&P và phối hợp việc kiểm soát và cân bằng để phê duyệt ngân sách.
3. Xây dựng lịch trình cho các hoạt động được xác định trong định nghĩa công việc và định nghĩa các cột mốc chính xác và có thể đo lường.
4. Định nghĩa lô-gic tổ chức và thứ tự của các hoạt động và nguồn lực cần thiết để tạo và quản lý BD-S&P.
5. Ước lượng thời gian của mỗi hoạt động và đưa chúng vào như một phần của lịch trình.
6. Điều chỉnh kế hoạch quản lý BD-S&P theo thông tin mới.
7. Điều chỉnh các hoạt động quản lý, lịch trình, phương hướng và mục tiêu để đáp ứng với thông tin mới.
8. Chuẩn bị các hành động quản lý thích ứng để đáp ứng với các vấn đề hoặc cơ hội mới.
9. Áp dụng kiến thức, hiểu biết và công nghệ mới góp phần đạt được các mục tiêu quản lý BD-S&P.

### Thực hiện quản lý BD-S&P

1. Thiết lập và ban hành định hướng quản lý dưới dạng các chỉ thị và hướng dẫn cho BD-S&P.
2. Chỉ định các nguồn lực cho tất cả các vai trò được xác định phù hợp với trình tự các nhiệm vụ cần được thực hiện.
3. Kích hoạt các hệ thống giám sát cần thiết để có thể nắm bắt thông tin hiệu suất công việc và dùng nó để kiểm soát việc phát triển BD-S&P.
4. Thực hiện các nhiệm vụ được định nghĩa trong kế hoạch quản lý BD-S&P để đạt được các mục tiêu BD-S&P.
5. Đánh giá các biện pháp quản lý BD-S&P, thông tin hiệu suất công việc, việc tận dụng nguồn lực, các rủi ro có thể xảy ra, các cơ hội mới và quản lý các thay đổi để cải thiện hiệu suất công việc.
6. Cung cấp thông tin liên quan cho tất cả các bên liên quan như đã nêu trong kế hoạch quản lý BD-S&P.
7. Liên tục xác nhận các kết quả thực hiện công việc phù hợp với các yêu cầu BD-S&P bao gồm cả các kết quả sai lệch và kết quả không cần thiết.
8. Bố trí các định hướng chiến lược cho BD-S&P nhằm giải quyết các quyết định chính sách.
9. Thiết lập các kế hoạch riêng lẻ cho việc phát triển hoặc sửa đổi BD-S&P.
10. Quản lý các quyết định về BD-S&P.
11. Quản lý các rủi ro liên quan đến quản lý BD-S&P.
12. Quản lý các thay đổi đối với BD-S&P.

### Giám sát tính hiệu quả của BD-S&P

1. Giám sát và kiểm soát thực hiện công việc bằng cách theo dõi, xem xét và điều chỉnh tiến độ để đạt được các mục tiêu quản lý theo kế hoạch quản lý BD-S&P.
2. Giám sát hiệu suất công việc để xác định sự thay đổi so với kế hoạch quản lý BD-S&P.
3. Giám sát việc quản lý các vấn đề và hành động phòng ngừa trước các vấn đề có thể xảy ra.
4. Giám sát tiến độ thực hiện kế hoạch quản lý so với dự toán lịch trình
5. Giám sát tình trạng của BD-S&P (sử dụng các biện pháp quản lý đã được xác định) và xác định bất kỳ khu vực nào cần thêm sự chú ý.
6. Giám sát tình trạng phạm vi BD-S&P và quản lý các thay đổi so với phạm vị cơ sở.
7. Giám sát tình trạng lịch trình quản lý BD-S&P và quản lý các thay đổi so với lịch trình cơ sở.
8. Đánh giá kết quả thực tế so với mục tiêu đã hoạch định và thực hiện các hành động khắc phục khi cần thiết.
9. Thu thập và truyền đạt thông tin về hiệu suất cho tất cả các bên liên quan theo định kỳ.
10. Duy trì thông tin chính xác và kịp thời liên quan đến BD-S&P.
11. Đánh giá việc đạt được các mục tiêu quản lý BD-S&P định kỳ.
12. Cung cấp các dự báo để cập nhật thông tin lịch trình hiện tại.
13. Định nghĩa các hành động và đánh giá đảm báo chất lượng để xác nhận việc thực hiện các kế hoạch quản lý BD-S&P.
14. Báo các các kế hoạch và tình trạng quản lý BD-S&P phù hợp với các yêu cầu báo cáo.
15. Đánh giá và kiểm soát nỗ lực quản lý BD-S&P.

### Cập nhật kế hoạch quản lý BD-S&P

1. Hoàn thành kế hoạch quản lý BD-S&P trước đó.
2. Xem xét tất cả các thông tin để khẳng định công việc quản lý BD-S&P là hoàn thành và các mục tiêu BD-S&P được đáp ứng.
3. Giám sát và đánh giá các chỉ số cho nỗ lực quản lý BD-S&P.
4. Giả định sự tuân thủ với các quy định và tiêu chuẩn ảnh hưởng đến BD-S&P.
5. Thiết lập các thủ tục để điều tra và nắm bắt các lý do khác nhau cho các hành động quản lý được thực hiện như một phần của quản lý BD-S&P.
6. Ghi lại các bài học kinh nghiệm và truyền đạt cho tất cả các bên có liên quan.
7. Đóng góp các phương pháp tốt nhất cho quản lý BD-S&P.
8. Xem xét kỹ lưỡng tính hiệu quả của các phương pháp tiếp cận quản lý đã được áp dụng để giải quyết vấn đề quản lý BD-S&P.
9. Xác định các thay đổi cần được thực hiện đối với kế hoạch BD-S&P.
10. Lựa chọn các thay đổi cần được thực hiện trong lần lặp lại tiếp theo của kế hoạch quản lý BD-S&P.
11. Kết hợp các thay đổi vào kế hoạch quản lý BD-S&P.

## Hoạt động vận hành

### Hoạt động thiết kế giải pháp BD-S&P

#### Mục đích

Mục đích của các hoạt động thiết kế giải pháp BD-S&P là để xác định các giải pháp BD-S&P nhằm giải quyết các mối quan tâm của bên liên quan, đạt được các mục tiêu BD-S&P và đáp ứng được các yêu cầu liên quan.

CHÚ THÍCH 1: Một khía cạnh quan trọng của thiết kế giải pháp BD-S&P là cho phép các nhà phân tích và các bên liên quan hiểu được không gian trao đổi của các lựa chọn tiềm năng mà có thể đáp ứng được các mục tiêu (xem điểm 6.3.1.7 để biết thêm thông tin về bản chất của không gian trao đổi). Thông thường, một sự kết hợp đa dạng và khác biệt các giải pháp BD-S&P được xem xét để cho phép đánh đổi giữa các ràng buộc và mối quan tâm. Nói cách khác, trong việc xử lý một không gian vấn đề phức tạp, việc khám phá toàn bộ không gian giải pháp là cần thiết, như là một phần của hoạt động thiết kế giải pháp BD-S&P để cuối cùng có thể chọn ra được giải phải thích hợp nhất.

CHÚ THÍCH 2: (Các) giải pháp BD-S&P được lựa chọn có thể được dẫn xuất từ hoặc có thể là (các) giải pháp BD-S&P hiện có dưới sự giám sát của quản lý BD-S&P hoặc từ các nguồn khác.

#### Chuẩn bị và lập kế hoạch cho nỗ lực thiết kế giải pháp BD-S&P

1. Xác định (các) lĩnh vực vấn đề tiềm năng mà cần được giải quyết.
2. Định nghĩa mục đích dự kiến, phạm vi, mục tiêu và mức độ chi tiết nỗ lực thiết kế giải pháp BD-S&P.
3. Định nghĩa một hoặc nhiều hơn các cách tiếp cận thiết kế giải pháp BD-S&P phù hợp với các định hướng quản lý và quản trị BD-S&P và phù hợp với mục đích, phạm vi mà các mục tiêu của nỗ lực này.
4. Lựa chọn hoặc phát triển các kỹ thuật, phương pháp và công cụ cần thiết cho thiết kế giải pháp BD-S&P.
5. Lập kế hoạch cho nỗ lực thiết kế giải pháp BD-S&P.
6. Thiết lập phạm vi nỗ lực thiết kế giải pháp BD-S&P.
7. Thiết lập các chỉ số nỗ lực thiết kế giải pháp BD-S&P.

CHÚ THÍCH 1: Tại mức tối thiểu, các chỉ số và tiêu chí cho phép nhóm thiết kế giải pháp BD-S&P xác định thời điểm hoàn thành nhiệm vụ thiết kế giải pháp BD-S&P cần được thiết lập.

1. Xác định thông tin và dữ liệu cần thiết cho nỗ lực thiết kế giải pháp BD-S&P.
2. Có được quyền truy cập và các bên hỗ trợ cần thiết cho nỗ lực thiết kế giải pháp BD-S&P.

CHÚ THÍCH 2: Các bên hỗ trợ thường được lấy từ các hoạt động hỗ trợ giải pháp BD-S&P. Khi có được bên hỗ trợ từ các nguồn khác, chúng có thể trở thành các bên hỗ trợ ứng viên để sử dụng trong các dự án khác thông qua các hoạt động hỗ trợ giải pháp BD-S&P.

1. Xác định và định nghĩa các yếu tố công việc thiết kế giải pháp BD-S&P và các nguồn lực liên quan.
2. Phát triển lịch trình thiết kế giải pháp BD-S&P và định nghĩa các cột mốc liên quan.
3. Có được các phê duyệt và kinh phí cho kế hoạch.
4. Thu thập thông tin và dữ liệu cần thiết cho nỗ lực thiết kế giải pháp BD-S&P.
5. Đảm bảo nhân lực được đào tạo sử dụng các kỹ thuật, phương pháp và công cụ đã được xác định.

#### Giám sát, đánh giá và kiểm soát các hoạt động thiết kế giải pháp BD-S&P

1. Báo các các kế hoạch và tình trạng hoạt động thiết kế giải pháp BD-S&P.
2. Giám sát và theo dõi việc tuân thủ các chỉ thị và hướng dẫn quản trị BD-S&P.
3. Giám sát và theo dõi việc tuân thủ các chỉ dẫn và hướng dẫn quản lý BD-S&P.
4. Giám sát và theo dõi các chỉ số nỗ lực thiết kế giải pháp BD-S&P.
5. Xác định và đánh giá các rủi ro và cơ hội liên quan đến nỗ lực thiết kế giải pháp BD-S&P.
6. Duy trì khả năng truy xuất các kết quả thiết kế giải pháp BD-S&P đến các tài liệu nguồn được sử dụng trong các hoạt động.
7. Thực thi các hành động khắc phục để sửa đổi kế hoạch công việc hoặc tổ chức lại công việc với kế hoạch.
8. Đánh giá và kiếm soát nỗ lực thiết kế giải pháp BD-S&P.

#### Mô tả đặc điểm không gian vấn đề và các vấn đề liên quan

1. Xác định (các) tình huống hiện tại và dự kiến trong không gian vấn đề.

CHÚ THÍCH 1: Không gian vấn đề và không gian giải pháp là trừu tượng. Tuy nhiên bản thân vấn đề và giải pháp lại có thể thực tế hoặc quan sát được, và chúng có thể là vô hình hoặc hữu hình. Ví dụ như vấn đề có thể là làm việc không hiệu quả (thực tế và quan sát được) và giải pháp là sử dụng các máy móc nhanh hơn (hữu hình) hoặc áp dụng các quy trình tốt hơn (vô hình). Nói theo cách, không gian vấn đề liên quan đến một thế giới của các thách thức và động lực của người dùng – tất cả là về vấn đề các nhu cầu (trạng thái cảm thấy thiếu thốn). Không gian giải pháp liên quan đến thế giới của các sản phẩm, dịch vụ và công nghệ - tất cả là về vấn đề đáp ứng nhu cầu.

1. Xác định các vấn đề khó khăn và cơ hội trong (các) tình huống hiện tại và tương lai.

CHÚ THÍCH 2: Khái niệm “vấn đề” được sử dụng theo trong ISO/IEC/ IEEE 15288: “khó khăn, không chắc chắn, sự kiện được phát hiện và không mong muốn, tập hợp các sự kiện, điều kiện hoặc tình huống mà cần phải có sự điều tra và hành động khắc phục”. Một không gian vấn đề là một sư biểu diễn tinh thần của một vấn đề (hoặc một tập các vấn đề) chứa kiến thức về trạng bái ban đầu và trạng thái mục tiêu của (các) vấn đề cũng như các trạng thái trung gian mà cần được tìm kiếm để có thể liên kết phần đầu và phần cuối của nhiệm vụ.

1. Xác định các khía cạnh liên quan của (các) tính huống được xác định.

CHÚ THÍCH 3: Một khía cạnh là cách một sự vật có thể được nhìn nhận hoặc được xem xét, một cách giải thích hoặc một quan điểm khác. Sự hiểu biết rõ ràng về các khía cạnh khác nhau có liên quan có thể giúp đảm bảo việc hiểu rõ toàn bộ bản chất của các vấn đề, khó khăn và cơ hội. Một lỗi phổ biến là không xem xét những vấn đề này từ các khía cạnh nhau.

1. Kiểm tra nhu cầu nhiệm vụ và nghiệp vụ hiện tai và tương lai đối với các vấn đề, khó khăn và cơ hội này.
2. Xác định các bên liên quan và mối quan tâm của họ tương ứng với các vấn đê, khó khăn và cơ hội này.
3. Xác định và phân tích bất ký các yêu cầu chính thức hoặc không chính thức áp dụng cho tình huống này và lưu văn bản các yêu cầu nào có liên quan đến nỗ lực hiện tại và cách thức chúng áp dụng cho tiêu chí đánh giá.
4. Xác định các thuộc tính chất lượng liên quan đến các mối quan tâm của các bên liên quan.
5. Xác định và mô tả đặc điểm cách mà các vấn đề, khó khăn và cơ hội ảnh hướng đến các bên liên quan khác nhau và các ưu tiên của họ trong việc giải quyết các vấn đề này.
6. Xác định và mô tả đặc điểm các phức tạp của từng vấn đề, khó khăn và cơ hội, nguyên nhân và kết quả của nó, và cách giải quyết hiện tại từng vấn đề trong các tình huống được xác định.

#### Thiết lập các mục tiêu và tiêu chí đánh giá giải pháp BD-S&P

1. Thu thập, phân tích và thương lượng các yêu cầu liên quan cho từng vấn đề, khó khăn và cơ hội được xác định.
2. Xác định các điều kiện ranh giới, nguyên nhân gốc, định hướng và các kịch bản liên quan cho từng vấn đề, khó khăn và cơ hội được xác định.
3. Xác định các lỗ hổng và thiếu sót của các giải pháp hiện tại hoặc được lên kế hoạch trong việc giải quyết vấn đề.
4. Xác định các giả thuyết, mức độ tự do, ràng buộc, điều kiện và thách thức liên quan.
5. Xác định và mô tả các mối quan hệ nguyên nhân và kết quả đối với (các) vấn đề hoặc khó khăn đã được xác định.

CHÚ THÍCH: Các mạng suy luận có thể được dùng để mô tả đặc điểm các mối quan hệ nguyên nhân – kết quả và có thể có nhiều hình dạng dựa trên các tình huống như là cây vấn đề, sơ đồ ảnh hưởng, mạng Bayesian, sơ đồ vòng lặp nguyên nhân – kết quả, sơ đồ xương cá,...

1. Hình thành một tuyên bố rõ ràng cho (các) vấn đề và (các) cơ hội.
2. Xác định và định nghĩa các mục tiêu giải pháp BD-S&P giải quyết (các) vấn đề liên quan đến các mối quan tâm, yêu cầu, hoặc các thuộc tính chất lượng của các bên liên quan, hoặc tận dụng lợi thế của các cơ hội được xác định.
3. Định nghĩa các tiêu chí đánh giá có thể được sử dụng để đánh giá mức độ giải quyết vấn đề và để cung cấp thông tin cho việc thăm dò và lựa chọn giải pháp thay thế.

CHÚ THÍCH: Các tiêu chí đánh giá này liên quan trực tiếp đến các khía cạnh của (các) vấn đề trong không gian vấn đề và chủ yếu quan tâm đến việc đạt được “mục địch cuối cùng” mong muốn. Do đó chúng đôi khi được gọi là mục tiêu cuối cùng. Trong một số lĩnh vực, mục tiêu cuối cùng liên quan trực tiếp đến “hiệu quả” mong muốn và là cơ sở cho việc phân tích dựa trên kết quả. Các tiêu chí này là khác nhau nhưng liên quan đến “mục tiêu phương tiện” được định nghĩa trong phân tích không gian giải pháp.

#### Tổng hợp (các) giải pháp tiềm năng trong không gian giải pháp

1. Phát triên một góc nhìn khách quan bằng việc định dạng lại các yếu tố trong đặc tính nguyên nhân – kết quả như là các điều kiện và mức độ cần đạt được trong việc giải quyết các vấn đề được phát hiện trong quá trình kiểm tra đặc tính này.
2. Xác định các chiến lược giảm thiểu vấn đề có thể đạt được các điều kiện và mức độ trên và đóng vai trò như là (các) giải pháp tiềm năng.
3. Thực hiện rà quét công nghệ đối với các công nghệ liên quan.
4. Thực hiện rà quét mẫu vấn đề/giải pháp cho các giải pháp liên quan đối với các vấn đề tương tự.
5. Thực hiện rà quét ẩn dụ hệ thống tự nhiên để tìm các giải pháp tự nhiên xảy ra cho các vấn đề tương tự.
6. Thực hiện đánh giá rủi ro cho các chiến lược được xác định.
7. Xác định các giải pháp tồn tại hoặc trước đó để làm rõ xem liệu chúng có thể được dùng như là (các) giải pháp tiềm năng cho tình huống đang được kiểm hiện tại hoặc được dự báo tra hay không.

CHÚ THÍCH 1: Các giải pháp có thể được tìm thấy trong các giải pháp BD-S&P hiện tại hoặc tương lai và đôi khi có thể giải quyết cho một hoặc nhiều vấn đề hoặc khó khăn.

1. Xem xét các mối quan hệ kết quả giữa các chiến lược giảm thiểu vấn đề và các nguyên nhân gây ra vấn đề để đảm bảo tình hoàn thiện của (các) giải pháp tiềm năng.

CHÚ THÍCH 2: Các chiến lượng có thể áp dung cho nhiều mục tiêu khác nhau. Điều quan trọng là phải làm rõ các mối quan hệ giữa các chiến lược và các mục tiêu để tạo điều kiện thuận lới cho việc kiểm tra tính hoàn chỉnh của giải pháp.

1. Xây dựng (các) tuyên bố mục đich cho từng giải pháp tiềm năng.

CHÚ THÍCH 3: Có thể có các tuyên bố mục đích khác nhau cho từng giải pháp vì giải pháp có thể không giải quyết toan bộ vấn đề hoặc toàn bộ khía cạnh của vấn đề.

1. Xác định các nhu cầu, mong muốn và kỳ vọng cho từng giải pháp tiềm năng.

CHÚ THÍCH 4: Kỳ vọng là cái mà người nào đó coi là có khả năng xảy ra, không liên quan gì đến cái mà người đó cần hoặc mong muốn. Kỳ vọng có thể thúc đẩy các giải pháp nhiều như những gì mà một người cần hoặc mong muốn.

1. Xác định các yếu tố thành công quan trọng liên quan và chỉ số hoạt động chính cho mỗi giải pháp tiềm năng.

CHÚ THÍCH 5: Các yếu tố thành công có thể khác nhau đối với mỗi giải pháp tiềm năng. Các yếu tố này phụ thuộc vào góc độ vấn đề mà giải pháp dựa trên. Các yếu tố thành công có liên quan tới mục đích của giải pháp cụ thể đó. Các giải pháp được đề xuất cũng có thể giải quyết các khía cạnh/phần khác nhau của vấn đề. Các yếu tố thành công và chỉ số hoạt động có thể dựa trên các mối quan tâm của các bên liên quan được xác định hoặc các thuộc tính chất lượng từ việc phân tích không gian vấn đề.

#### Mô tả đặc điểm các giải pháp và không gian trao đổi

CHÚ THÍCH 1: Không gian trao đổi là phạm vi và mức độ các thông số, tính chất và đặc điểm cần để thỏa mãn các mục tiêu giải pháp BD-S&P và các mối quan tâm các bên liên quan. Phân tích không gian trao đổi được sử dụng để phân tích các ràng buộc, điều kiện và thách thức liên quan đến các vấn đề phực tạp lớn với nhiều bên liên quan và nhiều mục tiêu. Nó liên quan đến việc xác định và hiểu về sự đánh đổi liên quan đến việc lựa chọn giữa các giải pháp cạnh tranh.

1. Kiểm tra bối cảnh mà các bên liên quan nhìn nhận giá trị và hình thành các đề xuất giá trị cho từng giải pháp tiềm năng.
2. Xác định các điểm mạnh, điểm yếu, cơ hội và mối đe dọa cho từng giải pháp tiềm năng.
3. Xác định các khía cạnh quan trọng khác liên quan đến từng giải pháp tiềm năng bao gồm nhưng không giới hạn các vấn đề sau.
4. Xác định và mô tả đặc điểm các rủi ro cho từng giải pháp tiềm năng.
5. Xác định các giả định đối với từng giải pháp tiềm năng.
6. Xác định các vấn đề bổ sung có thể gây ra bởi các giải pháp tiềm năng.
7. Xác định các khoảng trống hoặc thiếu hụt sau khi thực hiện các giải pháp tiềm năng.
8. Kết hợp hài hòa các yếu tố của từng giải pháp để đảm bảo rằng nó thể được thực hiện một cách chặt chẽ và gắn kết.
9. Xác định và mô tả đặc điểm các sự đánh đổi giữa và bên trong các giải pháp được đề xuất.

CHÚ THÍCH 2: Các sự đánh đổi có thể là bên trong hoặc giữa các giải pháp. Cũng có các sự đánh đổi giữa các giải pháp đề xuất và hiện trạng (có thể được coi như là một trong những “giải pháp” thay thế được xem xét). Những đánh đổi điển hình cần xem xét là: chi phí so với hiệu suất, chi phí so với lịch trình, dung lượng so với tốc độ chuyển đổi, độ chính xác so với mốc thời gian, chi phí mua lại so với chi phí vận hành, dễ sử dụng so với bảo mật, linh hoạt so với dự đoán, nhanh nhẹn so với mạnh mẽ, rủi ro so với phần thưởng,…

1. Xác định và mô tả đặc điểm các ảnh hưởng tiêu cực và tích cực và các tương tác giữa các giải pháp đề xuất và các giải pháp sẵn có/đã được lập kế hoạch.
2. Hình thành một lộ trình thực hiện (các) giải pháp đề xuất.
3. Định nghĩa các tiêu chí đánh giá được dùng để đánh giá mức độ (các) giải pháp giải quyết (các) vấn đề cụ thể và để cung cấp thông tin cho việc thăm dò và lựa chọn giải pháp thay thế.

CHÚ THÍCH 3: Các tiêu chí đánh giá này liên quan trực tiếp đến các khía cạnh của (các) giải pháp trong không gian giải pháp và chủ yếu quan tâm đến “phương tiên” mà giải pháp dùng để giải quyết các vấn đề được xác định. Như vậy, chúng đôi khi được gọi là mục tiêu phương tiện. Các tiêu chí này là khác nhau nhưng liên quan đến “các mục tiêu cuối cùng” được định nghĩa trong quá trình phân tích không gian vấn đề.

#### Hình thành (các) giải pháp BD-S&P ứng viên

1. Thiết lập và nắm bắt các đặc điểm chức năng và phi chức năng mong muốn dựa trên (các) giải pháp tiềm năng liên quan đến mục đích của từng giải pháp tương ứng với các mối quan tâm bên liên quan, các yêu cầu và ràng buộc liên quan và các thuộc tính chất lượng được xác định trong quá trình phân tích không gian vấn đề.
2. Tạo ra các khái niệm và thuộc tính cấu trúc, hành vi và tổ chức nhằm hỗ trợ các đặc điểm chức năng và phi chức năng.

VÍ DỤ 1: Các khái niệm và thuộc tính này có thể được thể hiện dưới dạng các cấu trúc có dạng công nghệ thông tin như là luồng thông tin, luồng điều khiển, các cấu trúc dữ liệu, các quy tắc hoạt động, các biểu đồ sự kiện/dấu vết, các biểu đồ chuyển trạng thái, mốc thời gian, lộ trình,…

VÍ DỤ 2: Các khái niệm và thuộc tính này có thể được thể hiện dưới các dạng khác như là các mô hình rủi ro, mô hình tài chính, mô hình kinh tế, mô hình mô phỏng, mô hình độ nhạy, mô hình xếp hàng (cũng như các loại mô hình mô phỏng sự kiện liên tục và rời rạc khác), mô hình không gian địa lý, mô hình quản lý, mô hình nghiệp vụ, mô hình tác động xã hội và môi trường, mô hình dòng giá trị,...

1. Xác định và mô tả đặc điểm các sự đánh đổi giữa các giải pháp BD-S&P ứng viên.
2. Xác định các đặc điểm chính cung cấp các hiểu biết chi tiết cho vấn đề BD-S&P và dùng chúng để định nghĩa bối cảnh và phạm vi của các giải pháp BD-S&P.

CHÚ THÍCH 1: Các đặc điểm này dựa trên các mối quan tâm bên liên quan, các yêu cầu liên quan, các thuộc tính chất lượng, các mục tiêu BD-S&P và các yếu tố khác có liên quan được xác định. Một ánh xạ giữa các định hướng và các đặc điểm như vậy có thể được phát triển để hỗ trợ việc truy xuất nguồn gốc.

1. Hình thành các nguyên tắc, hướng dẫn, giao thức và tiêu chuẩn cho từng giải pháp BD-S&P ứng viên.
2. Phân tích và phân bổ các đặc điểm cho các thành phần và quy trình tạo nên từng giải pháp BD-S&P.
3. Xác định các quy trình và hoạt động cung cấp hoặc kích hoạt các đặc điểm được xác định khi được sắp xếp hoặc được thực hiện theo một trình tự cụ thể
4. Xác định các quy tắc chi phối các thành phần, cấu tạo của chúng, sự tương tác và sự phụ thuộc lẫn nhau nhằm đảm bảo rằng mỗi giải pháp BD-S&P ứng viên cung cấp hoặc kích hoạt các đặc điểm mong muốn.
5. Đảm bảo mỗi giải pháp BD-S&P ứng viên cung cấp các đặc điểm mong muốn hoặc đảm bảo chúng có thể thực hiện được.
6. Xác định các vấn đề và khu vực cần cải thiện trong (các) quá trình BD-S&P.
7. Nếu có nhiều hơn một giải pháp BD-S&P thì lựa chọn giải (các) giải pháp tốt nhất để sử dụng cho luồng đường xuống.

CHÚ THÍCH 2: Các hoạt động đánh giá giải pháp BD-S&P có thể được sử dụng để tạo điều kiện thuận lợi cho việc lựa chọn các giải pháp BD-S&P phù hợp nhất. Các kết quả phân tích không gian vấn đề có thể được sử dụng như một cơ sở cho các tiêu chí đánh giá. Thông thường, việc sàn lọc ban đầu các giải pháp BD-S&P ứng viên được thực hiện trước khi gửi các đánh giá này để tránh việc các nỗ lực không cần thiết trong việc đánh giá các ứng viên như là trùng lặp, tốn kém hoặc rủi ro, không phù hợp hoặc không khả thi,…

CHÚ THÍCH 3: Trong một số trường hợp, việc lựa chọn (các) giải pháp BD-S&P sau này được thực hiện thông qua các quyết định nằm ngoài phạm vị của hoạt động thiết kế giải pháp BD-S&P. Trong trường hợp này, các giải pháp BD-S&P ứng viên sẽ được trình bày cho những người ra quyết định cùng với đánh giá về các giải pháp BD-S&P này.

### Các hoạt động đánh giá giải pháp BD-S&P

#### Mục đích

Mục đích của các hoạt động đánh giá giải pháp BD-S&P là để làm rõ mức độ mà một hoặc nhiều giải pháp BD-S&P đáp ứng được các mục tiêu BD-S&P và giải quyết được các mối quan tâm bên liên quan, hoặc làm rõ chất lượng hoặc tính hoàn chỉnh của BD-S&P.

#### Chuẩn bị và lên kế hoạch nỗ lực đánh giá giải pháp BD-S&P

1. Xác định (các) quyết định tiềm năng có thể được giải quyết bằng nỗ lực đánh giải giải pháp BD-S&P.
2. Định nghĩa các mục đích, phạm vi, mục tiêu và mức độ chi tiết dự kiến của nỗ lực đánh giá giải pháp BD-S&P.
3. Xem xét mục đích, phạm vi và các mục tiêu được nêu của nỗ lực đánh giá giải pháp BD-S&P với bên tài trợ, bên thiết kế và các bên quan tâm khác.
4. Xác định một hoặc nhiều cách tiếp cận đánh giá giải pháp BD-S&P phù hợp với các định hướng quản lý và quản trị BD-S&P và phù hợp với mục đích, phạm vi và các mục tiêu cho nỗ lực này.
5. Lựa chọn và phát triển các kỹ thuật, phương thức và công cụ cần thiết cho đánh giá giải pháp BD-S&P.
6. Lựa chọn và phát triển một khung đánh giá giải pháp BD-S&P.
7. Thu thập bất kỳ yêu đầu quy định nào có liên quan.
8. Lập kế hoạch nỗ lực đánh giá giải pháp BD-S&P.
9. Thiết lập phạm vi cho nỗ lực đánh giá giải pháp BD-S&P.
10. Thiết lập chỉ số cho nỗ lực đánh giá giải pháp BD-S&P.
11. Xác định thông tin và dữ liệu cần thiết cho nỗ lực đánh giá giải pháp BD-S&P.
12. Có được quyền truy cập các bên hỗ trợ cần thiết cho nỗ lực đánh giá giải pháp BD-S&P.

CHÚ THÍCH: Các bên hỗ trợ thường được chỉ ra từ các hoạt động hỗ trợ giải pháp BD-S&P. Khi có được các bên hỗ trợ từ các nguồn khác, chúng có thể trở thành bên hỗ trợ ứng viên để sử dụng trong các dự án khác thông qua các hoạt động hỗ trợ giải pháp BD-S&P.

1. Xác định và định nghĩa các yếu tố công việc đánh giá giải pháp BD-S&P và các nguồn lực liên quan.
2. Phát triển lịch trình đánh giá giải pháp BD-S&P và định nghĩa các cột mốc liên quan.
3. Có được các phê duyệt và kinh phí cần thiết cho kế hoạch.
4. Thu thập thông tin và dữ liệu cần thiết cho nỗ lực đánh giá giải pháp BD-S&P.
5. Đảm bảo nhân lực được đào tạo sử dụng các kỹ thuật, phương pháp và công cụ được xác định.
6. Đảm bảo nhân lực có quyền truy cập cần thiết và thích hợp đến các sản phẩm công việc giải pháp BD-S&P.

#### Giám sát, đánh giá và kiểm soát các hoạt động đánh giá giải pháp BD-S&P

1. Báo cáo các kế hoạch và tình trạng hoạt động đánh giá giải pháp BD-S&P.
2. Giám sát và đánh giá việc tuân thủ các chỉ thị và hướng dẫn quản trị BD-S&P.
3. Giám sát và đánh giá việc tuân thủ các chỉ thị và hướng dẫn quản lý BD-S&P.
4. Giám sát và đánh giá các thông số cho nỗ lực đánh giá giải pháp BD-S&P.
5. Xác nhận và đánh giá các rủi ro và cơ hội liên quan đến nỗ lực đánh giá giải pháp BD-S&P.
6. Duy trì khả năng truy xuất nguồn gốc các kết quả đánh giá giải pháp BD-S&P tới tài liệu nguồn được sử dụng trong các hoạt động.
7. Đảm bảo khả năng truy xuất nguồn gốc và tích hợp của thông tin được đánh giá.
8. Thực hiện các hành động khắc phục để sửa đổi kế hoạch hoặc sắp xếp lại công việc theo kế hoạch.
9. Đánh giá và kiểm soát nỗ lực đánh giá giải pháp BD-S&P.
10. Quản lý các rủi ro liên quan đến đánh giá giải pháp BD-S&P.

#### Xác định các tiêu chí đánh giá

CHÚ THÍCH 1: Các tiêu chí đánh giá bao gồm cả tiêu chí đánh giá giá trị và tiêu chí phân tích thuộc tính.

CHÚ THÍCH 2: Các mục tiêu đánh giá có thể liên quan hoặc không liên quan đến các mục tiêu được sử dụng trong thiết kế giải pháp BD-S&P. Trong mọi trường hợp thì các mục tiêu thiết kế cần được kiểm tra để xác đinh xem chúng áp dụng vào đánh giá này tại mức độ nào.

CHÚ THÍCH 3: Tiêu chí đánh giá có thể dựa trên các kết quả từ việc thực hiện phân tích không gian vấn đề trong quy trình thiết kế giải pháp BD-S&P hoặc quy trình khác.

1. Xác định các chỉ thị và mệnh lệnh, bao gồm cả các chính sách và tiêu chuẩn có liên quan.
2. Xác định các bên liên quan và mối quan tâm của họ đối với (các) giải pháp BD-S&P được đánh giá.

CHÚ THÍCH 4: Các mối quan tâm của bên liên quan được xem xét trong quy trình đánh giá giải pháp BD-S&P có thể khác so với các mối quan tâm của bên liên quan được giải quyết trong thiết kế (các) giải pháp BD-S&P ban đầu. Ví dụ như là việc đánh giá có thể được giao nhiệm vụ xác định giải pháp BD-S&P có phù hợp với một số mục đích khác được hình dung ban đầu hay là không.

1. Định nghĩa các tiêu chí đánh giá giá trị đóng góp vào các yếu tố thành công, các chỉ số chính và các quyết định cần phải đưa ra.

CHÚ THÍCH 5: Trong quá trình đánh giá giải pháp BD-S&P, các tiêu chí đánh giá giá trị được định nghĩa trong quá trình thiết kế giải pháp BD-S&P có thể được đánh giá về mức độ phù hợp cho nỗ lực đánh giá và nếu cần thiết thì có thể đưa thêm các tiêu chí hoặc các tiêu chí tồn tại có thể được chỉnh sửa để phản ánh bối cảnh đánh giá.

1. Định nghĩa tiêu chí phân tích thuộc tính để hỗ trợ tiêu chí đánh giá giá trị.

CHÚ THÍCH 6: Coi các thuộc tính chất lượng đã được thống nhất cho giải pháp BD-S&P như là các ứng viên cho tiêu chí phân tích thuộc tính.

1. Xác định các mối quan hệ giữa tiêu chí đánh giá giá trị và tiêu chí phân tích thuộc tính.

CHÚ THÍCH 7: Các mối quan hệ giữa tiêu chí đánh giá giá trị và tiêu chí phân tích thuộc tính được xem xét khi các kết quả của việc phân tích được sử dụng để xác định mức độ giải quyết các mối quan tâm của bên liên quan. Các quan hệ này thường được cấu trúc để tạo điều kiện cho việc thực hiện đánh giá giá trị và liên hệ với các kết quả phân tích.

1. Xác đinh các mối quan hệ giữa tiêu chí đánh giá giá trị, tiêu chí phân tích thuộc tính và các yếu tố của giá trị và tiện ích (ví dụ: hàm giá trị, đường cong tiện ích).

CHÚ THÍCH 8: Nhiệm vụ này xác định cách mà hai bộ tiêu chí ánh xạ tới “các đường cong giá trị” biểu thi các số liệu có giá trị cho giải pháp BD-S&P.

#### Xác định các phương pháp đánh giá và tích hợp với các mục tiêu và tiêu chí đánh giá

1. Lựa chọn hoặc phát triển các phương pháp phân tích thuộc tính và đánh giá giá trị để hỗ trợ các tiêu chí phân tích thuộc tính và đánh giá giá trị được xác định.

CHÚ THÍCH 1: Các phương pháp này có thể được phát triên bởi các hoạt động hỗ trợ giải pháp BD-S&P. Nếu vậy thì chúng sẽ được đặt trong kho giải pháp BD-S&P. Nếu như các phương thức này được phát triển tại đây thì chúng có thể được cung cấp cho việc hỗ trợ giải pháp BD-S&P như là các hạng mục ứng viên để được làm phù hợp việc tái sử dụng trong tổ chức.

1. Xem xét các mục tiêu, tiêu chí và phương pháp đánh giá và phân tích và các thang đo, trọng số liên quan (nếu có) với nhà tài trợ và nhà thiết kế.
2. Xác định các nguồn thông tin để sử dụng trong quá trình áp dụng các tiêu chí phân tích thuộc tính và đánh giá giá trị.

CHÚ THÍCH 2: Một số thông tin có được từ việc phân tích nhưng số khác có được từ các nguồn khác như là các nỗ lực đánh giá trước đó, kinh nghiệm vận hành, cơ sở dữ liệu ngành, các hoạt động xác thực hệ thống và các hoạt động nghiên cứu.

#### Thiết lập các kỹ thuật, phương pháp và công cụ đo lường

CHÚ THÍCH 1: Nhiều đánh giá giải pháp BD-S&P có thể được thực hiện đầy đủ mà không cần phải huy động một cấu trúc đa lớp đáng kế của các lớp phân tích thuộc tính và đánh giá giá trị. Tại mức tối thiểu, quy trình đánh giá từng phương án thay thế so với các tiêu chí. Quy trình này không cần lúc nào cũng phải định lượng và không phải lúc nào cũng áp dụng cho các thang đo lường. Các trọng số không hoàn toàn bắt buộc do đây là vấn đề đa mục tiêu và mục đích là thường để trình bày cho các bên liên quan về sự đánh đổi giữa các mục tiêu đó, chứ không nhất thiết phải xác định về mặt toán học các giải pháp “tốt nhất”.

1. Tận dụng các thang đo và trọng số như là phương tiên đo lường các yếu tố và tính chất của giải pháp BD-S&P khi thích hợp.
2. Định nghĩa các thang đo phân tích để đo lường dựa trên các tiêu chí phân tích khi thích hợp.
3. Định nghĩa các thang đo đánh giá để đo lường dựa trên các tiêu chí đánh giá khi thích hợp.
4. Làm rõ các trọng số cho các tiêu chí phân tích và đánh giá khi thích hợp.

CHÚ THÍCH 2: Một số phương pháp không sử dụng các trọng số, trong khi số khác dựa trên chúng để đạt được các kết quả chính xác hơn. Có các loại trọng số khác nhau như là trọng số quan trọng, trọng số xoay, trọng số tới hạn. Các phương pháp được chọn thường làm rõ các loại trọng số được sử dụng.

1. Xác định ví trí hiện tại của giải pháp BD-S&P trên cân đo và xác định (các) điểm mong muốn cho các mức thành tự trong tương lai.
2. Xác định các thước đo thích hợp cho các thuộc tính giải pháp BD-S&P liên quan.
3. Xác định các chỉ số cần được định rõ từ các thước đo.

CHÚ THÍCH 3: Có sự chồng chéo giữa các thước đo và các chỉ số. Cả hai đều có thể là định tính hoặc định lượng, nhưng sự khác biệt mới là quan trọng. Các thước đo là cụ thể, thường đo một thứ và có bản chất định lượng (ví dụ như tôi có năm quả táo). Các chỉ số mô tả chất lượng và yêu cầu một cơ sở đo lường (Tôi có nhiều hơn năm quả táo so với hôm qua). Thước đo và chỉ số có thể hữu dụng trong việc thiết lập các ưu tiên của chương trình, phân bổ nguồn lực và đo lường hiệu suất.

1. Định nghĩa các mối quan hệ giữa các thước đo, chỉ số và tiêu chí đo lường.
2. Xác định các nguồn thông tin để thu được các giá trị cho các thước đo và chỉ số này.
3. Xác định các kỹ thuật, phương pháp và công cụ thích hợp cho các thước đo, chỉ số và tiêu chí đánh giá này.
4. Ước lượng độ chính xác, sai số và mức độ không đảm bảo của kết quả khi sử dụng các thước đo, chỉ số và tiêu chí đánh giá này.

#### Xem xét thông tin liên quan đến hoạt động đánh giá

1. Xác định các thông tin có liên quan cho các phương pháp phân tích thuộc tính và đánh giá giá trị được chọn.

CHÚ THÍCH 1: Nếu có thể, tái sử dụng các dữ liệu và kết quả từ các lần đánh giá trước thuộc loại này nếu như thông tin hiện có vẫn còn giá trị.

1. Thu thập các thông tin liên quan và cần thiết.
2. Tạo các thông tin bổ sung nếu không có sẵn (nghĩa là không tồn tại, không tiếp cận được), nếu việc tạo thông tin là khả thi trong thời gian sẵn có mà không gây gián đoạn.
3. Kiểm tra và giám định các thành phần lạ về tính đầy đủ, đúng đắn và thống nhất.
4. Phát triển một sự hiểu biết về giải pháp BD-S&P, các thuộc tính chất lượng giải pháp BD-S&P, các quyết định chính và các mối quan tâm của hệ thống.

CHÚ THÍCH 2: Các thuộc tính chất lượng có thể được định nghĩa để mô tả đặc điểm cách giải quyết các mối quan tâm của bên liên quan.

#### Phân tích các thuộc tính giải pháp BD-S&P và đánh giá giá trị các bên liên quan

1. Xác định các giải pháp thay thế cho việc đánh giá giải pháp BD-S&P nếu thích hợp.

CHÚ THÍCH 1: Các giải pháp thay thế có thể đến từ các hoạt động thiết kế giải pháp BD-S&P.

CHÚ THÍCH 2: Hiện trạng đôi khi là một trong nhưng giải pháp thay thế được xem xét.

CHÚ THÍCH 3: Việc phát triển các giải pháp thay thế này có thể nằm ngoài phạm vị của hoạt động đánh giá. Tuy nhiên, đôi khi hoạt động đánh giá xác định rằng không có đủ số lượng, sự đa dạng, hoặc mức độ mà các giải pháp thay thế này được định nghĩa trước và cần có thêm các giải pháp thay thế bổ sung.

CHÚ THÍCH 4: Loại bỏ các giải pháp thay thế giống nhau và giải pháp không cung cấp được các trường hợp phân biệt ứng với tiêu chí đánh giá.

1. Sử dụng (các) phương pháp phân tích và đánh giá như đã nêu trong kế hoạch công việc đánh giá để đánh giá giải pháp BD-S&P cho một mục đích đã xác định.
2. Sử dụng các phương thức đánh giá để xác định các khái niệm và thuộc tính của giải pháp BD-S&P (thay thế) ứng với tiêu chí đánh giá.

VÍ DỤ: Các ví dụ về các phương thức để xác định các khái niệm và thuộc tính này bao gồm các yêu tố như là phân tích, quan sát, giả lập, tạo bản mẫu, thử nghiệm, điều tra, kiểm toán, xem xét, xem qua và đánh giá của chuyên gia.

1. Đánh giá giải pháp BD-S&P và các giải pháp thay thế dựa trên các thuộc tính chất lượng, các mối quan tâm của bên liên quan và các mục tiêu giải pháp BD-S&P được xác định.
2. Xác định và mô tả đặc điểm các chi phí, rủi ro và cơ hội.

CHÚ THÍCH 5: Các rủi ro đã được xác định trong quá trình thiết kế giải pháp BD-S&P cho từng giải pháp tiềm năng đang được xem xét. Các rủi ro được xác định ở đây cho giải pháp BD-S&P đang được đánh giá có thể liên quan đến các rủi ro đã được xác định trước đó.

1. Mô tả đặc điểm độ chính xác, các mức độ không đảm bảo liên quan đến mức độ sai số của các phép đo được sử dụng và trong các kết qủa khác đo được trong quá trình đánh giá.

#### Mô tả đặc điểm (các) giải pháp BD-S&P dựa trên các kết quả đánh giá

1. Xác định và mô tả đặc điểm các sự đánh đối ứng với các thuộc tính chất lượng, các mối quan tâm của bên liên quan, các thuộc tính giải pháp BD-S&P, các chi phí, rủi ro và cơ hội.
2. Đánh giá mức độ đáp ứng bao gồm các chính sách, tiêu chuẩn, các nhiệm vụ và mệnh lệnh liên quan, của (các) giải pháp BD-S&P

CHÚ THÍCH 1: Trong một số trường hợp, giải pháp BD-S&P đáp ứng được các mục tiêu và giải quyết được các mối quan tâm của bên liên quan nhưng lại không đáp ứng được nhiệm vụ và mệnh lệnh. Giải pháp này có thể được giảm bớt yêu cầu phải đáp ứng các nhiệm vụ hoặc mệnh lệnh đó, nhưng phải xem xét việc giảm bớt yêu cầu này có phù hợp hay không.

CHÚ THÍCH 2: Trong một số trường hợp, việc tốt hơn là loại bỏ sớm các giải pháp thay thế cho giải pháp BD-S&P không đáp ứng được các nhiệm vụ và mênh lệnh trong quá trình nhằm tránh tiêu tốn nguồn lực đáng kể trong việc đánh giá thêm các hạng mục này. Tuy nhiên, việc loại bỏ sớm cũng có thể hữu ích để xem xét còn bao xa chúng có thể đáp ứng được các nhiệm vụ và mệnh lệnh.

1. Đánh giá các kết quả của phân tích này để xác định một cách phù hợp (các) giải pháp thay thế tốt nhất, chất lượng của giải pháp BD-S&P, hoặc mức độ đáp ứng các mục tiêu giải pháp BD-S&P, đáp ứng các yêu cầu liên quan, hoặc thỏa mãn các mối quan tâm của bên liên quan của giải pháp BD-S&P.
2. Xem xét các kết quả phân tích và đánh giá với nhà tài trợ, nhà thiết kế và các bên quan tâm khác.

#### Hình thành các phát hiện và khuyến nghị

1. Xác định và mô tả đặc điểm các phát hiện từ việc đánh giá.
2. Phân tích các phát hiện.
3. Xác thực các phát hiện với các chuyên gia về chủ để liên quan và các bên liên quan khác.
4. Đánh giá các ý nghĩa của các phát hiện.
5. Phát triển các khuyến nghị.
6. Xem xét các phát hiện và các khuyến nghị cùng với nhà tài trợ, nhà thiết kế và các bên quan tâm khác.

#### Thu thập và truyền đạt các kết quả đánh giá

1. Xác định đối tượng truyền đạt các kết quả đánh giá.
2. Lựa chọn các phát hiện và khuyến nghị liên quan và chi tiết nhất.
3. Xây dựng một báo cáo đánh giá.
4. Có được sự chấp thuận cho báo cáo nếu phù hợp.
5. Trình bày các phát hiện và khuyến nghị tới những người ra quyết định nếu có liên quan.
6. Trình bày cho các nhà thiết kế và các bên liên quan chính.
7. Thu thập các ý kiến phàn hổi từ các bài thuyết trình này (ví dụ: các vấn đề, mục hành động, rủi ro, quan sát, quan điểm).
8. Nếu được yêu cầu hoặc đề nghị, lặp lại các phần có liên quan của việc đánh giá.
9. Nếu bản đánh giá được cập nhật, xem xét các thay đổi với nhà tài trợ, nhà thiết kế và các bên quan tâm khác.
10. Cập nhật báo cáo dựa trên các phản hồi từ các bài thuyết trình nếu cần thiết.
11. Lưu trữ bào cáo và các phàn hồi nhận được trong quá trình thuyết minh.

### Các hoạt động hỗ trợ giải pháp BD-S&P

#### Mục đích

Mục đích của các hoạt động hỗ trợ giải pháp BD-S&P là để phát triển, duy trì và cải thiện các năng lực và nguồn lực khả dụng cần thiết để thực hiện các giải pháp BD-S&P. Các hoạt động này cũng có thể liên quan đến việc đạt được hoặc phát triển các khả năng và tài nguyên này khi được yêu cầu.

#### Chuẩn bị và lập kế hoạch cho nỗ lực hỗ trợ giải pháp BD-S&P

1. Xác định năng lực và nguồn lực khả dụng cần thiết để hỗ trợ quản trị và quản lý BD-S&P.
2. Xác định các năng lực và nguồn lực khả dụng cần thiết để hỗ trợ thiết kế và đánh giá các giải pháp BD-S&P.
3. Xác định các hướng dẫn, chính sách, chiến lược và ràng buộc cho việc triển khai các năng lực và nguồn lực khả dụng.

CHÚ THÍCH: Những hướng dẫn, chính sách, chiến lược và ràng buộc này có thế có được từ các chỉ thị quản trị BD-S&P và hướng dẫn quản lý BD-S&P.

1. Xác định và định nghĩa các vai trò và trách nhiệm cần thiết của những người tham gia vào nỗ lực hỗ trợ giải pháp BD-S&P.
2. Lập kế hoạch cho nỗ lực hỗ trợ giải pháp BD-S&P
3. Thiết lập phạm vi cho nỗ lực hỗ trợ giải pháp BD-S&P.
4. Thiết lập các chỉ số cho nỗ lực hỗ trợ giải pháp BD-S&P.
5. Thu thập thông tin và dữ liệu cần thiết cho nỗ lực hỗ trợ giải pháp BD-S&P.
6. Có được quyền truy cập tới các khả năng và nguồn lực cần thiết cho nỗ lực hỗ trợ giải pháp BD-S&P.
7. Xác định và định nghĩa các yếu tố công việc hỗ trợ giải pháp BD-S&P và các nguồn lực liên quan.
8. Phát triển lịch trình hỗ trợ giải pháp BD-S&P và định nghĩa các cột mốc liên quan.
9. Phát triển các kế hoạch kiểm soát và truyền thông cần thiết cho hỗ trợ giải pháp BD-S&P.
10. Có được các phê duyệt và kính phí cho kế hoạch.

#### Giám sát, đánh giá và kiểm soát các hoạt động hỗ trợ giải pháp BD-S&P

1. Báo cáo các kế hoạch và tình trạng hoạt động hỗ trợ giải pháp BD-S&P.
2. Giám sát và đánh giá sự tuân thủ các hướng dẫn và chỉ thị quản trị BD-S&P của hỗ trợ giải pháp BD-S&P.
3. Giám sát và đánh giá sự tuân thủ các hướng dẫn và chỉ thị quản lý BD-S&P của hỗ trợ giải pháp BD-S&P.
4. Giám sát và đánh giá các chỉ số cho nỗ lực hỗ trợ giải pháp BD-S&P.
5. Xác định các vấn đề hỗ trợ phát sinh từ các thay đổi đối với cách tiếp cận giải pháp BD-S&P

CHÚ THÍCH: Ví dụ việc chuyển từ cách tiếp cận dựa trên chức năng sang hướng dịch vụ có thể dẫn tới một thay đổi đáng kể trong các hạng mục hỗ trợ giải pháp BD-S&P.

1. Xác định và đánh giá các rủi ro và cơ hội liên quan đến nỗ lực hỗ trợ giải pháp BD-S&P.
2. Giám sát và đánh giá việc sử dụng đúng cách các bên hỗ trợ giải pháp BD-S&P.
3. Giám sát và đánh giá việc sử dụng đúng cách các thư viện và kho giải pháp BD-S&P.
4. Thực hiện các hành động khắc phục để sửa đổi kế hoạch công việc hoặc sắp xếp lại công việc so với kế hoạch.
5. Đánh giá và kiểm soát nố lực hỗ trợ giải pháp BD-S&P.

#### Quản lý các bên hỗ trợ tiến trình giải pháp BD-S&P

1. Quản lý các quyết định về các bên hỗ trợ giải pháp BD-S&P sử dụng quy trình Quản lý Quyết định trong ISO/IEC /IEEE 15288 làm hướng dẫn.
2. Quản lý các rủi ro liên quan đến các bên hỗ trợ giải pháp BD-S&P sử dụng quy trình Quản lý Rủi ro trong ISO/IEC /IEEE 15288 làm hướng dẫn.
3. Quản lý các thay đổi trong các bên hỗ trợ giải pháp BD-S&P sử dụng quy trình Quản lý Cấu hình trong ISO/IEC /IEEE 15288 làm hướng dẫn.
4. Quản lý các kho, thư viện và cơ sở dữ liệu giải pháp BD-S&P sử dụng quy trình Quản lý Thông tin trong ISO/IEC /IEEE 15288 làm hướng dẫn.
5. Quản lý các kho, thư viện và cơ sở dữ liệu giải pháp BD-S&P sử dụng quy trình Quản lý Kiến thức trong ISO/IEC /IEEE 15288 làm hướng dẫn.
6. Quản lý chất lượng các bên hỗ trợ giải pháp BD-S&P sử dụng quy trình Quản lý Chất lượng trong ISO/IEC /IEEE 15288 làm hướng dẫn.
7. Quản lý hạ tầng liên quan đến các bên hỗ trợ giải pháp BD-S&P sử dụng quy trình Quản lý Hạ tầng trong ISO/IEC /IEEE 15288 làm hướng dẫn.

#### Phát triển và thiết lập các khả năng và nguồn lực khả dụng

1. Xác định các khả năng và nguồn lực có thể tận dụng để tạo điều kiện thuận lợi cho việc đạt được tầm nhìn, chiến lược, các mục đích và mục tiêu BD-S&P.
2. Phát triển một danh mục các khả năng và nguồn lực có thể được sử dụng bởi các hoạt động BD-S&P khác và đưa danh mục này vào cơ sở dữ liệu giải pháp BD-S&P.
3. Phát triển và thiết lập một kho giải pháp BD-S&P có thể được sử dụng để lưu trữ các thông tin và dữ liệu liên quan đến giải pháp BD-S&P.
4. Thiết lập các biện pháp kiểm soát truy cập đối với các thông tin và dữ liệu liên quan đến giải pháp BD-S&P trong kho giải pháp BD-S&P.
5. Thiết lập các mẫu sản phẩm công việc có thể sử dụng bởi các hoạt động BD-S&P khác.
6. Phát triển các thông tin cần thiết và luồng thông tin cần cho việc quản trị và quản lý BD-S&P.
7. Xác định các lĩnh vực cải tiến và đào tạo bổ sung để có thể thúc đẩy tầm nhìn, chiến lược, các mục đích và mục tiêu BD-S&P.
8. Thiết lập các dịch vụ, hoạt động, sự kiện và kiểm soát có thể áp dụng vào hỗ trợ giải pháp BD-S&P.

CHÚ THÍCH: Sự kiện là các mốc, xem xét, kiểm toán, điểm quyết định chính, cổng chất lượng,… Kiểm soát là các danh sách kiểm tra, tiêu chí đầu vào, tiêu chí đầu ra, cây quyết định,...

#### Triển khai các năng lực và nguồn lực để sử dụng cho các hoạt động BD-S&P khác

1. Triển khai các kho giải pháp BD-S&P để duy trì các sản phầm giải pháp BD-S&P.
2. Điều chỉnh các hoạt động, dịch vụ, nguồn lực, năng lực và thông tin một cách gắn kết nhằm cung cấp hỗ trợ giải pháp BD-S&P có hiệu quả.
3. Triển khai các năng lực, dịch vụ, hoạt động, sự kiện và điều khiển để hỗ trợ các hoạt động BD-S&P khác.
4. Triển khai các nguồn lực, năng lực, tài sản, hoạt động và dịch vụ tổ chức thích hợp nhằm cung cấp hỗ trợ giải pháp BD-S&P.
5. Triển khai các mẫu sản phẩm công việc giải pháp BD-S&P.
6. Triển khai các cấu trúc thông tin và các luồng thông tin cần thiết cho hỗ trợ giải pháp BD-S&P.
7. Triển khai các cơ chế nhằm thu thập các thông tin và dữ liệu liên quan cần thiết cho nỗ lực hỗ trợ giải pháp BD-S&P.
8. Triển khai các cơ chế nhằm thu thập các thông tin và dữ liệu liên quan cần thiết cho quản lý kho giải pháp BD-S&P.
9. Cung cấp đào tạo và chứng nhận năng lực và nguồn lực khả dụng.

#### Phát triển nguồn lực và năng lực hỗ trợ giải pháp BD-S&P

1. Xác định các khoảng trống và thiếu hụt nguồn lực và năng lực khả dụng.
2. Các cơ chế được sử dụng để thu thập thông tin và dữ liệu “có liên quan” hoặc “được sử dụng” trong hỗ trợ giải pháp BD-S&P.
3. Các nội dung và cấu trúc kho giải pháp BD-S&P.
4. Các nội dung và cấu trúc thư viện giải pháp BD-S&P.
5. Các nội dung và cấu trúc cơ sở dữ liệu giải pháp BD-S&P.
6. Các hướng dẫn và mẫu sản phẩm công việc.
7. Các luồng và cấu trúc thông tin liên quan đến việc thực hiện các hoạt động BD-S&P.
8. Các dịch vụ, hoạt động, sự kiện và kiểm soát hỗ trợ.
9. Các bên hỗ trợ quản trị BD-S&P.
10. Các bên hỗ trợ quản lý BD-S&P.
11. Các bên hỗ trợ thiết kế giải pháp BD-S&P.
12. Các bên hỗ trợ đánh giá giải pháp BD-S&P.
13. Kiểm tra những lỗ hổng và thiếu sót để xác định các cải tiến tiềm năng.
14. Đề xuất các cải tiến đối với hoạt động phát triển bên hỗ trợ.
15. Giám sát việc phát triển của các bên hỗ trợ được cải tiến để đảm bảo đạt được các cải tiến đúng như mong đợi.

## Các khía cạnh bảo mật và quyền riêng tư của các vai trò dữ liệu lớn

Tất cả các vai trò của dữ liệu lớn được định nghĩa trong TCVN ISO/IEC 20547-3:2022, bao gồm: nhà cung cấp chức năng dữ liệu lớn (BDFP), đối tác dịch vụ dữ liệu lớn (BDSP), người dùng dữ liệu lớn (BDC) và nhà cung cấp dữ liệu lớn (BDP) (xem mục 8, TCVN ISO/IEC 20547-3:2022) có các trách nhiệm duy trì bảo mật và quyển riêng tư (S&P) dữ liệu lớn. Như được thể hiện trong Hình 1, các khía cạnh S&P của các vai trò dữ liệu lớn là:

* Lập kế hoạch S&P dữ liệu lớn;
* Quản lý S&P dữ liệu lớn;
* Triển khai S&P dữ liệu lớn;
* Vận hành S&P dữ liệu lớn;
* Kiểm toán S&P dữ liệu lớn.



Hình 1 - Góc nhìn người dùng BDRA-S&P

Một tổ chức thường có cấu trúc ba lớp bao gồm lớp quản trị, lớp quản lý và lớp vận hành. Hình 2 thể hiện các vị trí của các khía cạnh S&P dữ liệu lớn trong cấu trúc ba lớp.



Hình 2 - Các khía cạnh S&P trong cấu trúc ba lớp tổ chức

Các hoạt động quản trị được miêu tả trong 6.1 được ánh xạ tới việc lập kế hoạch S&P dữ liệu lớn. Các hoạt động quản lý được miêu tả trong 6.2 được ánh xạ tới việc quản lý S&P dữ liệu lớn. Các hoạt động duy trì được miêu tả trong 6.3 được ánh xạ tới việc triển khai S&P dữ liệu lớn, vận hành S&P dữ liệu lớn và kiểm toán S&P dữ liệu lớn. Bảng 3 thể hiện các khía cạnh của S&P dữ liệu lớn và các hoạt động của chúng theo các ánh xạ này.

Bảng 3 - Các khía cạnh S&P dữ liệu lớn và các hoạt động của chúng

| **Các khía cạnh S&P** | **Khoản** | **Các hoạt động** | **Mục đích** |
| --- | --- | --- | --- |
| Lập kế hoạch S&P dữ liệu lớn | 6.1.2 | Chuẩn bị và lập kế hoạch cho nỗ lực quản trị S&P dữ liệu lớn | Để thiết lập và duy trì sự thống nhất và đồng bộ của BD-S&P với các mục tiêu và ràng buộc liên quan đến các nhu cầu bảo mật và quyền riêng tư hiện tại và tương lai của một tổ chức và các liên quan của tổ chức đó hoặc các nhóm quan tâm. |
| 6.1.3 | Giám sát, đánh giá và kiểm soát các hoạt động quản trị S&P dữ liệu lớn |
| 6.1.4 | Thiết lập các mục tiêu quản trị S&P dữ liệu lớn |
| 6.1.5 | Định hướng S&P dữ liệu lớn |
| 6.1.6 | Giám sát và đánh giá tính tuân thủ với các hướng dẫn và chỉ thị quản trị S&P dữ liệu lớn |
| 6.1.7 | Xem xét việc triển khai các hướng dẫn và chỉ thị quản trị S&P dữ liệu lớn và chuẩn bị cho sự thay đổi |
| Quản lý S&P dữ liệu lớn | 6.2.2 | Chuẩn bị và lập kế hoạch cho nố lực quản lý S&P dữ liệu lớn | Để đảm bảo việc thực thi đúng các chỉ thị quản trị BD-S&P và đạt được một cách hiệu quả và kịp thời các mục tiêu BD-S&P. |
| 6.2.3 | Giám sát, đánh giá và kiểm sát các hoạt động quản lý kiến trúc |
| 6.2.4  | Phát triển phương pháp tiếp cận quản lý S&P dữ liệu lớn |
| 6.2.5 | Thực hiện quản lý S&P dữ liệu lớn |
| 6.2.6 | Giám sát sự hiệu quả của S&P dữ liệu lớn |
| 6.2.7 | Cập nhật kế hoạch quản lý S&P dữ liệu lớn |
| Thực thi S&P dữ liệu lớn | 6.3.1.2 | Chuẩn bị và lập kế hoạch cho nỗ lực thiết kế giải pháp BD-S&P | Để xác định các giải pháp BD-S&P giải quyết các mối quan tâm của bên liên quan, đạt được các mục tiêu BD-S&P và đáp ứng được các yêu cầu liên quan. |
| 6.3.1.3 | Giám sát, đánh giá và kiểm soát các hoạt động thiết kế giải pháp BD-S&P |
| 6.3.1.4 | Mô tả đặc điểm không gian vấn đề và các vấn đề có liên quan |
| 6.3.5 | Thiết lập các mục tiêu giải pháp BD-S&P và tiêu chí đánh giá |
| 6.3.1.6 | Tổng hợp (các) giải pháp tiềm năng trong không gian giải pháp |
| 6.3.1.7 | Mô tả đặc điểm các giải pháp và không gian trao đổi |
| 6.3.1.8 | Hình thành (các) giải pháp BD-S&P ứng viên |
| Vận hành dữ liệu lớn | 6.3.3.2 | Chuẩn bị và lập kế hoạch cho nỗ lực hỗ trợ giải pháp BD-S&P | Để phát triển, duy trì và cả thiện các năng lực hỗ trợ và các nguồn lực cần thiết trong việc thực hiện các giải pháp BD-S&P. |
| 6.3.3.3 | Giám sát, đánh giá và kiểm soát các hoạt động hỗ trợ giải pháp BD-S&P  |
| 6.3.2.4 | Quản lý quy trình các bên hỗ trợ giải pháp BD-S&P |
| 6.3.3.5 | Phát triển và thiết lập các năng lực và nguồn lực khả dụng |
| 6.3.3.6 | Triển khai các năng lực và nguồn lực để sử dụng trong các hoạt động BD-S&P khác |
| 6.3.3.7 | Cải thiện các năng lực và nguồn lực hỗ trợ giải pháp BD-S&P |
| Kiểm toán S&P dữ liệu lớn | 6.3.2.2 | Chuẩn bị và lập kế hoạch cho nỗ lực đánh giá giải pháp BD-S&P | Để xác định mức độ một hoặc nhiều giải pháp BD-S&P đáp ứng được các mục tiêu và giải quyết các mối quan tâm của bên liên quan, hoặc xác định chất lượng và độ hoàn thiện của BD-S&P. |
| 6.3.2.3 | Giám sát, đánh giá và kiểm soát các hoạt động đánh giá giải pháp BD-S&P |
| 6.3.2.4 | Xác định các tiêu chí đánh giá |
| 6.3.2.5 | Xác định các phương pháp đánh giá và tích hợp với các tiêu chí và mục tiêu đánh giá |
| 6 3 2 6 | Thiết lập các kỹ thuật, phương pháp và công cụ đo lường |
| 6.3.2.7 | Xem xét các thông tin có liên quan đến việc đánh giá |
| 6.3.2.8 | Phân tích các thuộc tính giải pháp BD-S&P và đánh giá giá trị bên liên quan |
| 6.3.2.9 | Mô tả đặc điểm (các) giải pháp BD-S&P dựa trên các kết quả đánh giá |
| 6.3.2.10 | Hình thành các phát hiện và khuyến nghị |
| 6.3.2.11 | Thu thập và truyền đạt các kết quả đánh giá |

# Hướng dẫn về các hoạt động bảo mật và quyển riêng tư cho dữ liệu lớn

## Khái quát chung

Phần này này cung cấp các hướng dẫn về hoạt động bảo mật và quyền riêng tư liên quan đến các vai trò, hoạt động và các thành phần chức năng được định nghĩa ở trong BDRA.

Hình 3 mô tả các mối quan hệ giữa các tổ chức và BDRA:

* một tổ chức là một phần của hệ sinh thái tuân theo BDRA. BDRA bao gồm các vai trò và vai trò phụ, các hoạt động và thành phần chức năng;
* một tổ chức thực thi các hoạt động liên quan đến các vai trò, hoạt động và thành phần chức năng. Ví dụ, một tổ chức có thể phụ trách vai trò của nhà cung ứng dụng dữ liệu lớn; và
* một tổ chức thực hiện các hoạt động tập trung vào bảo mật và quyền riêng tư. Chúng được áp dụng để bảo vệ các tài sản trong BDRA khỏi các lỗ hổng bảo mật. Một số tài sản có thể riêng cho một tổ chức, ví dụ như thông tin nhạy cảm mang tính chất thương mại, trong khi những thông tin khác có thể được chia sẽ trong hệ sinh thái, ví dụ như là tập dữ liệu.



Hình 3 - Mối quan hệ giữa các tổ chức và BDRA

Như được thể hiện trong Hình 4, khoản này tập trung vào hai loại hoạt động bảo mật và quyền riêng tư:

* các hoạt động tổ chức; và
* các hoạt động công tác hệ sinh thái.



Hình 4 - Hai góc nhìn về các hoạt động bảo mật và quyền riêng tư

## Hướng dẫn ở mức tổ chức

### Khái quát chung

Hình 5 thể hiện các tiêu chuẩn khác nhau có thể được sử dụng để hướng dẫn các tổ chức về các hoạt động bảo mật và quyền riêng tư dữ liệu lớn. Có bốn giai đoạn quan trọng:

* giai đoạn yêu cầu;
* giai đoạn phân tích rủi ro;
* giai đoạn kiểm soát thiết kế; và
* giai đoạn kỹ thuật vòng đời.



Hình 5 - Các tiêu chuẩn cho các hoạt động bảo mật và quyền riêng tư

### Hướng dẫn tiêu chuẩn cho các yêu cầu

Các hoạt động bảo mật và quyền riêng tư dữ liệu lớn xử lý các yêu cầu theo các tiêu chuẩn:

* tiêu chuẩn bảo mật của hệ thống dữ liệu lớn như được mô tả trong ISO/ IEC 27001;
* các yêu cầu bảo mật theo các lĩnh vực cụ thể của các hệ thống thông tin dữ liệu lớn như được mô tả trong ISO/IEC 27009;
* các yêu cầu quyền riêng tư của các hệ thống dữ liệu lớn đúc rút từ việc sử dụng các chính sách quyền riêng tư như được mô tả trong ISO/IEC 29100;
* các yêu cầu quyền riêng tư của các hệ thống thông tin dữ liệu lớn như được mô tả trong ISO/IEC 27701.

### Hướng dẫn tiêu chuẩn cho quản lý rủi ro

Các hoạt động bảo mật và quyền riêng tư dữ liệu lớn xử lý phân tích rủi ro theo các tiêu chuẩn sau:

* quản lý rủi ro bảo mật thông tin như được mô tả trong ISO/IEC 27005;
* các hướng dẫn đánh giá tác động quyền riêng tư như được mô tả trong ISO/IEC 29134.

### Hướng dẫn tiêu chuẩn cho các kiểm soát

Các hoạt động bảo mật và quyền riêng tử xử lý phân tích rủi ro theo các tiêu chuẩn sau:

* quy tắc thực hiện cho kiểm soát bảo mật thông tin như được mô tả trong ISO/IEC 27002;
* quy tắc thực hiện cho bảo vệ PII như được mô tả trong ISO/IEC 29151;
* các kỹ thuật khử nhận dạng dữ liệu nâng cao quyền riêng tư như được mô tả trong ISO/IEC 20899.

### Hướng dẫn tiêu chuẩn cho các hoạt động vòng đời

Các hoạt động bảo mật và quyền riêng tư dữ liệu lớn xử lý kỹ thuật vòng đời theo các tiêu chuẩn sau:

* kỹ thuật bảo mật như được mô tả trong ISO/ IEC 21827;
* kỹ thuật quyền riêng tư như được mô tả trong ISO/IEC 27550.

## Hướng dẫn ở mức hệ sinh thái

### Khái quát chung

Một tổ chức có thể phụ trách:

* Các vai trò BDRA, ví dụ như nhà cung cấp dữ liệu lớn, nhà cung cấp ứng dụng dữ liệu lớn, người dùng dữ liệu lớn;
* Các vai trò BDRA phụ, ví dụ như nhà cung cấp dịch vụ thu thập dữ liệu lớn, nhà cung cấp dịch vụ phân tích dữ liệu lớn, là các vai trò phụ của nhà cung cấp ứng dụng dữ liệu lớn;
* Cung cấp các thành phần chức năng BDRA. Chúng có thể là:
* các thành thành phần trong một lớp kiến trúc BDRA, ví dụ như năng lực phát trực tuyến trong lớp xử lý, hoặc một thành phần trực quan hóa trong lớp nền tảng; hoặc
* các thành phần trong phần các chức năng đa lớp của kiến trúc BDRA, ví dụ như năng lực xác thực; và
* Sự kết hợp các vai trò, vai trò phụ và cung cấp các thành phần chưc năng.

Bảo mật và quyền riêng tư có thể liên quan đến tài sản toàn cầu được chia sẻ bởi các tổ chức trong cùng một hệ sinh thái dữ liệu lớn. Trong trường hợp đó, các hoạt động bảo mật và quyền riêng tư có thể được điều phối như được thể hiện trong Hình 6:

* Mỗi tổ chức thực hiện các hoạt động bảo mật và quyền riêng tư của mình;
* Việc phối hợp tổng thể các hoạt động bảo mật và quyền riêng tư của các tổ chức đảm bảo tính nhất quán.



Hình 6 - Phối hợp các hoạt động bảo mật và quyền riêng tư

Sự phối hợp có thể dưới các hình thức khác nhau, ví dụ như một cơ quan công quyền, một tổ chức chuyên dụng, một liên minh. Dưới đây là các ví dụ về phối hợp quản lý bảo mật và quyền riêng tư:

* Các tổ chức liên quan đến dữ liệu lớn lưu lượng giao thông mà cho phép phân tích lưu lượng thông minh áp dụng các hoạt động bảo mật và quyền riêng tư có thể được điều phối bởi chính quyền thành phố;
* Các tổ chức liên quan đến dữ liệu lớn chăm sóc sức khỏe mà cho phép phân tích lâm sàng áp dụng các hoạt động bảo mật và quyền riêng tư có thể được điều phối bởi cơ quan sức khỏe quốc gia.;
* Các tổ chức liên quan đến dữ liệu lớn bảo hiểm mà cho phép phân tích rủi ro bảo hiểm áp dụng các hoạt động bảo mật và quyền riêng tư có thể được điều phối bới nhóm làm việc đặc biệt;

Điều khoản phụ này cung cấp các hướng dẫn cho việc phối hợp của các hoạt động bảo mật và quyền riêng tư sau đây trong các hệ sinh thái dữ liệu lớn:

* Chia sẻ dữ liệu, thuộc về loại quản lý kỹ thuật (ISO/IEC/IEEE 15288);
* Phân tích bảo mật và rủi ro, thuộc về loại quản lý kỹ thuật (ISO/IEC/IEEE 15288);
* Quản lý vòng đời, thuộc về loại quản lý kỹ thuật (ISO/IEC/IEEE 15288).

### Hướng dẫn chuỗi xử lý dữ liệu

Cần có sự phối hợp khi chuỗi xử lý dữ liệu đang hoạt động. Ví dụ, nhà vận hành hệ thống IoT có thể thu thập dữ liệu được cung cấp dưới dạng một tập dữ liệu cho các nhà cung cấp dịch vụ, mà từ đó kết hợp dữ liệu này với các nguồn dữ liệu khác và cung cấp cho người sử dụng dữ liệu. Như được thể hiện trong Hình 7:

* Mỗi tổ chức thực hiện các hoạt động chia sẻ dữ liệu của mình;
* Sự phối hơp tổng thể của các hoạt động chia sẻ dữ liệu của mỗi tổ chức đảm bảo tính bảo mật và quyền riêng tư của chuỗi xử lý dữ liệu.



Hình 7 - Phối hợp chuỗi xử lý dữ liệu

Các hướng dẫn sau được cung cấp:

* Ở mức độ hệ sinh thái:
* xác định các yêu cầu hoạt động chuỗi xử lý dữ liệu như là tốc độ chuyển đổi, tính xác thực, khả năng mở rộng, nguồn gốc xuất xứ;
* xác định các yêu cầu bảo vệ tính bảo mật và quyền riêng tư của chuỗi xử lý dữ liệu như là tính bí mật, tính toàn vẹn, tính sẵn sàng, tính không liên kết, tính minh bạch và khả năng can thiệp của dữ liệu;
* xác định các yêu cầu cụ thể liên quan đến các vai trò, vai trò phụ, hoạt động và các thành phần chức năng BDRA; và
* thiết lập các kế hoạch thực hiện phối hợp bảo mật và quyền riêng tư trong hệ sinh thái, bao gồm các biện pháp cho việc thực hành tuân thủ, đảm bảo và kiểm toán.
* Ở mức độ tổ chức:
* xác định các yêu cầu hoạt động tổ chức cụ thể như là tốc độ chuyên đổi, tính xác thực, khả năng mở rộng, nguồn gốc xuất xứ;
* xác định các yêu cầu bảo vệ tính bảo mật và quyền riêng tư tổ chức cụ thể về tính bí mật, tính toàn vẹn, tính sẵn sàng, tính không liên kết, tính minh bạch và khả năng can thiệp của dữ liệu;
* thiết lập các hoạt động chia sẽ dữ liệu phù hợp với hệ thống phối hợp hệ sinh thái.

### Hướng dẫn quản lý rủi ro

Cần có sự phối hợp cho việc quản lý rủi ro. Ví dụ, nếu dữ liệu được thu thập bởi nhà vận hành hệ thống IoT và được cung cấp dưới dạng một tập dữ liệu cho nhà cung cấp dịch vụ bị xâm phạm thì các hoạt động của nhà cung cấp dịch vụ cũng bị xâm phạm. Như được thể hiện trong Hình 8:

* mỗi tổ chức thực hiện các hoạt động quản lý rủi ro bảo mật và quyền riêng tư của mình;
* phối hợp tổng thể của việc quản lý rủi ro bảo mật và quyền riêng tư đảm bảo một sự hiểu biết chung về các rủi ro ở mức độ hệ sinh thái;



Hình 8 - Phối hợp quản lý rủi ro bảo mật và quyền riêng tư

Hướng dẫn sau được cung cấp:

* Tại mức độ hệ sinh thái:
* xác định các lỗ hổng và mối nguy ở mức độ hệ sinh thài cần đến một sự phối hợp. Khuyến cáo rằng các tổ chức trong hệ sinh thái cần cung cấp các mô tả dựa trên các phân loại chung. Phụ lục A đưa ra ví dụ như là các phân loại STRIDE và LINDDUN.
* xác định các rủi ro và vi phạm của hệ sinh thái;
* xác định các kiểm soát để xử lý các rủi ro của hệ sinh thái;
* xác định các yêu cầu quản lý rủi ro bảo mật và quyền riêng tư liên quan đến các vai trò, vai trò phụ, hoạt động và thành phần chức năng BDRA; và
* thiết lập các kế hoạch thực hiện phối hợp quản lý rủi ro bảo mật và quyền riêng tư trong hệ sinh thái, bao gồm các biện pháp cho việc giám sát rủi ro và cho việc thực hành tuân thủ, đảm bảo và kiểm toán.
* Tại mức độ tổ chức:
* xác định các lỗ hổng và mối nguy của hệ thống mà tổ chức chịu trách nhiệm trong hệ sinh thái;
* xác định các rủi ro và vi phạm của hệ thống;
* xác định các kiểm soát để xử lý các rủi ro của hệ thống;
* thiết lập các hoạt động quản lý rủi ro bảo mật và quyền riêng tư phù hợp với kế hoạch thực hiện phối hợp hệ sinh thái

### Hướng dẫn các hoạt động vòng đời

Cần có sự phối hợp trong vòng đời bảo mật và quyền riêng tư của dữ liệu lớn. Ví dụ,

* Các tổ chức có thể thống nhất việc sử dụng các kiểm soát như là:
* mức độ bảo vệ đã thống nhất cho dữ liệu ở trạng thái nghỉ;
* mức độ toàn vẹn và xác thực đã thống nhất cho dữ liệu ở trạng thái động;
* mức độ sẵn sàng đã thống nhất cho việc xử lý dữ liệu;
* mức độ không liên kết đã thống nhất cho nguồn gốc dữ liệu.
* Các tổ chức có thể thống nhất sự phối hợp đối với quản lý sự cố, như là:
* mức độ chuẩn bị sẵn sàng đã thống nhất;
* một cơ chế cảnh báo chung cho các vi phạm bảo mật (ví dụ: phát hiện sự giả mạo) hoặc các vị phạm quyền riêng tư (ví dụ: phát hiện sự tái nhận dạng).

Như được thể hiện trong Hình 9:

* Mỗi tổ chức thực hiện các hoạt động vòng đời bảo mật và quyền riêng tư của mình;
* Phối hợp tổng thể của vòng đời bảo mật và quyền riêng tư đảm bảo việc xử lý nhất quán các tài sản cần được bảo vệ.



Hình 9 - Phối hợp vòng đời bảo mật và quyền riêng tư

Hướng dẫn sau được cung cấp:

* Tại mức độ hệ sinh thái:
* xác định các hoạt động trong vòng đời hệ sinh thái tại nơi cần đến sự phối hợp (sự đảm bảo, sự xác minh tuân thủ, quản lý sự cố, kiểm toán);
* xác định các kiểm soát được cần được thực thi hơn nữa trong hệ sinh thái cho việc phối hợp phân tích rủi ro. Khuyến cáo rằng các tổ chức trong hệ sinh thái cần cung cấp các mô tả dựa trên các phân loại chung. Thí dụ mục lục B cung cấp phân loại sử dụng trong ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29151;
* thiết lập các kế hoạch thực hiện phối hợp kiểm soát trong hệ sinh thái bao gồm các kiểm soát tính tuân thủ, tính đảm bảo và kiểm toán.
* Tại mức độ tổ chức:
* xác định các hoạt động trong vòng đời hệ thống nơi các mối quan tâm về bảo mật và quyền riêng tư cần được tích hợp;
* xác định các kiểm soát cần được thực thi hơn nữa trong hệ thống cho việc phân tích rủi ro;
* thiết lập các hoạt động vòng đời phù hợp với kế hoạch thực hiện phối hợp hệ sinh thái.

Phụ lục C cung cấp các ví dụ như sự phối hợp hệ sinh thái và kết quả của các hoạt động bảo mật và quyền riêng tư.

# Các thành phần chức năng bảo mật và quyền riêng tư

## Tổng quan

Điều 7 mô tả BDRA-S&P dưới dạng các tập hợp chung các thành phần chức năng. Một thành phần chức năng là một yếu tố chức năng của BDRA-S&P được sử dụng để thực hiện một hoạt động hoặc các phần của một hoạt động và có một thành phần thực thi trong việc thực hiện cụ thể một kiến trúc.

Các kiểm soát bảo mật và quyền riêng tư trong các tiêu chuẩn hiện hành có thể được tận dụng để hiện thực hóa các thành phần chức năng bảo mật và quyền riêng tư với việc xem xét bổ sung các mục tiêu bảo mật và quyền riêng tư trong bối cảnh dữ liệu lớn. Phụ lục B liệt kê các danh mục mục tiêu bảo mật và quyền riêng tư được nêu cụ thể trong ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29151.

## Các thành phần chức năng cho cả bảo mật và quyền riêng tư

Các danh mục kiểm soát bảo mật được nêu rõ trong ISO/IEC 27002 được sử dụng trong tài liệu này như là các thành phần chức năng cho cả bảo mật và quyền riêng tư như sau:

1. **Các chính sách bảo mật thông tin** để cung cấp các định hướng quản lý và hỗ trợ cho an toàn thông tin phù hợp với các yêu cầu nghiệp vụ và xem xét sự tuân thủ các quy định và luật pháp có liên quan.
2. **Tổ chức bảo mật thông tin** để thiết lập các khung quản lý nhằm khởi tạo và kiểm soát việc thực thi các hoạt động an toàn thông tin trong tổ chức.
3. **Bảo mậ nguồn nhân lực** để đảm bảo các nhân viên và nhà thầu hiểu rõ được trách nhiệm của họ và phù hợp với các vai trò mà họ được xem xét trước quá trình công tác, để đảm bảo các nhân viên và nhà thầu nhận thực được việc hoàn thành trách nhiệm bảo mật thông tin của họ trong quá trình công tác, để bảo vệ các lợi ích của tổ chức như một phần của quá trình thay đổi hay chấm dứt công tác khi có sự thay đổi và chấm dứt công tác.
4. **Quản lý tài sản** để xác định các tài sản tổ chức và định nghĩa các trách nhiệm bảo vệ thích hợp, để đảm bảo thông tin nhận được một mức độ bảo vệ thích hợp phù hợp với mức độ quan trọng của quản lý đối với tổ chức theo phân loại thông tin, để ngăn chặn sự tiết lộ thông tin, thay đổi, loại bỏ hoặc phả hủy trái phép thông tin lưu trữ trên phương tiện truyền thông.
5. **Kiểm soát truy cập** để gới hạn quyền truy cập tới thông tin và các phương tiện xử lý thông tin, để đảm bảo người dùng được phép truy cập và ngăn chặn truy cập trái phép vào các hệ thống và dịch vụ, để khiến người dùng có trách nhiệm với việc bảo vệ thông tin xác thực của họ, để ngăn chặn truy cập trái phép vào các hệ thống và ứng dụng.
6. **Mật mã** để đảm báo việc dùng mật mã chính xác và hiệu quả để bảo vệ tính bí mật, tính xác thực và/hoặc tính toàn vẹn của thông tin.
7. **Bảo mật môi trường và vật lý** để đảm bảo các truy cập vật lý trái phép, gây thiệt hại và trở ngại cho thông tin và các phương tiên xử lý thông tin của tổ chức, để ngăn chặn mất mát, hư hỏng, mất cắp hoặc xâm phạm các tài sản và gián đoạn đến các hoạt động của tổ chức.
8. **Hoạt động bảo mật** để đảm bảo các hoạt động an toàn và chính xác của các phương tiện xử lý thông tin, để đảm bảo thông tin và các phương tiện xử lý thông tin được bảo vệ khỏi phần mềm độc hại, để bảo vệ khỏi sự mất mát của dữ liệu bằng việc sao lưu dự phòng, để ghi lại các sự kiện và tạo bằng chứng bằng cách giám sát và ghi nhật ký, để đảm bảo tính toàn vẹn của hệ thống vận hành bằng việc kiểm soát phần mềm vận hành, để ngăn chặn việc khai thác các lỗ hổng kỹ thuật, để giảm thiểu sự tác động của các hoạt động kiểm toán đối với các hệ thống vận hành.
9. **Bảo mật thông tin liên lạc** để đảm bảo sự bảo vệ các thông tin trong các mạng lưới và phương tiện xử lý thông tin hỗ trợ cho các mạng đó, để duy trì bảo mật thông tin được di chuyển bên trong tổ chức và tới bất kỳ thực thể bên ngoài nào.
10. **Tiếp nhận, phát triển và duy trì hệ thống** để đảm bảo rằng bảo mật thông tin là một phần không thể thiếu của các hệ thống thông tin trong toàn bộ vòng đời (bao gồm cả các yêu cầu đối với các hệ thống thông tin cung cấp các dịch vụ qua các mạng công cộng), để đảm bảo bảo mật thông tin được thiết kế và thực thi trong vòng đời phát triển của các hệ thống thông tin, để đảm bảo sự bảo vệ các dữ liệu được sử dụng cho kiểm thử.
11. **Các mối quan hệ với các nhà cung cấp** để đảm bảo sự bảo vệ các tài sản của tổ chức có thể tiếp cận được bởi các nhà cung cấp, để duy trì mức độ bảo mật thông tin đã thống nhất và cung cấp dịch vụ phù hợp với các thỏa thuận của nhà cung cấp.
12. **Quản lý sự cố bảo mật thông tin** để đảm bảo cách tiếp cận nhất quán và hiệu quả việc quản lý các sự cố bảo mật thông tin, bao gồm cả việc truyền đạt các sự kiện và điểm yếu bảo mật.
13. **Các khía cạnh bảo mật thông tin của việc quản lý tính liên tục trong nghiệp vụ** cần được đưa vào trong các hệ thống quản lý tính liên tục trong nghiệp vụ của tổ chức, để đảm bảo tính sẵn sàng của của các phương tiện xử lý thông tin bằng phương pháp dự phòng.
14. **Sự tuân thủ** luật pháp, luật định, quy định và các tuân thủ hợp đồng liên quan đến bảo mật thông tin và của bất kỳ các yêu cầu bảo mật nào được giả định trước, để đảm bảo bảo mật thông tin được thực thi và vận hành phù hợp với các chính sách và quy trình tổ chức.

Phụ lục D cung cấp ví dụ như các kiểm soát bảo mật và quyền riêng tư cho nhà cung cấp ứng dụng dữ liệu lớn (BDAP) và nhà cung cấp dữ liệu lớn (BDP).

## Các thành phần chức năng cho quyền riêng tư

Các danh mục kiểm soát quyền riêng tư cho các nhà kiểm soát PII và nhà xử lý PII được nêu rõ trong ISO/IEC 27701 được sử dụng trong tài liệu này như là các thành phần chức năng cho quyền riêng tư như sau:

1. **Các điều kiện đối với việc thu thập và xử lý** để xác định và làm tài liệu chứng minh rằng việc xử lý là hợp pháp, có cơ sở pháp lý theo các thẩm quyền hiện hành và với các mục đích được định nghĩa rõ ràng và hợp pháp.
2. **Quyền của các chủ PII** để đảm bảo các chủ PII được cung cấp thông tin thích hợp về việc xử lý PII của họ và đáp ứng bất kỳ nghĩa vụ hiện hành nào đối với các chủ PII liên quan đến việc xử lý PII của họ.
3. **Quyền riêng tư mặc định và bám sát thiết kế** đối với những người kiểm soát PII để đảm bảo các quá trình và hệ thống được thiết kế sao cho việc thu thập và xử lý PII (bao gồm cả sử dụng, tiết lộ, lưu giữ, truyền tải và loại bỏ) được giới hạn bằng yếu tố cần thiết cho mục đích được xác định.
4. **Chia sẻ, chuyển nhượng và tiết lộ PII** để xác định việc có hay không và lưu tài liệu việc chia sẻ, chuyển nhượng tới các bên thẩm quyền hoặc bên thứ ba và/hoặc tiết lộ PII theo các nghĩa vụ hiện hành.

Các khía cạnh khác để quan sát các thành phần chức năng cho quyền riêng tư như sau:

1. **Thực thi chính sách quyền riêng tư**

Một tổ chức như nhà kiểm soát PII nên định nghĩa chính sách quyền riêng tư của họ, cách họ bảo vệ dữ liệu cá nhân trong tổ chức, trong quá trình phát triển sản phẩm,... Chính sách quyền riêng tư có thể bao gồm chính sách phân loại dữ liệu cá nhân, đánh giá rủi ro quyền riêng tư, chia sẽ dữ liệu và các cơ chế bảo vệ được yêu cầu cần thiết trong vòng đời dữ liệu. Các cơ chế bảo vệ bao gồm chính sách mã hóa, khử nhận dạng, kiểm soát truy cập,... Khuyến nghị sử dụng các công cụ CNTT và mở rộng hệ thông bảo mật CBTT hiện có để thực thi chinh sách quyền riêng tư để việc dữ liệu cá nhân được bảo vệ đúng theo chính sách và việc vi pháp chính sách có thể được phát hiện.

1. **Phát hiện và kiểm kê dữ liệu cá nhân**

Thành phần này có thể phát hiện dữ liệu cá nhân trong kho dữ liệu hoặc trước quá trình truyền và thu thập dữ liệu. Việc phát hiện dữ liệu cá nhân trong dữ liệu phi cấu trúc như là văn bản, tệp âm thành và video phụ thuộc vào các phương pháp học máy và dựa trên luật lệ. Nguồn dữ liệu cá nhân cần được ghi lại. Dữ liệu cần phải được phân loại và gắn thẻ dựa trên độ nhạy cảm của chúng. Thêm nữa, dữ liệu thuộc về cùng các chủ thể dữ liệu cần được kiểm kê, điều này có thể tạo thuận lợi cho việc quản lý dữ liệu cá nhân. Trong mọi trường hợp một chủ thể dữ liệu yêu cầu xóa dữ liệu cá nhân của họ, dữ liệu có liên quan vẫn có thể dễ dàng được tìm thấy.

1. **Khử nhận dạng**

Thành phần này có thể thay đổi dữ liệu cá nhân để danh tính của các chủ thể dữ liệu được ẩn đi. Việc này giảm thiểu tính nhạy cảm của dữ liệu cá nhân theo nghĩa là nó sẽ khó khăn trong việc liên kết với chủ thể dữ liệu hoặc giảm lượng thông tin hiển thị về chủ thể dữ liệu. Thành phần này cũng dự trữ các tiện ích ở một mức độ nhất định để đáp ứng các yêu cầu nghiệp vụ. Các công nghệ thường được sử dụng cho việc khử nhận dạng các tập dữ liệu có cấu trúc được mô tả trong ISO/IEC 20889 2018. Việc lựa chọn các công nghệ dựa trên các rủi ro quyền riêng tư của các tình huống nhất định và chính sách quyền riêng tư được định nghĩa của tập đoàn. Cần phải có sự đánh đổi giữa bảo vệ quyền riêng tư và tiên ích dữ liệu. Các công nghệ khử nhận dạng cần được áp dụng càng sớm càng tốt trong vòng đời của dữ liệu để giảm thiểu các rủi ro quyền riêng tư ở các bước xử lý tiếp theo. Các công nghệ cần hỗ trợ các ứng dụng có quy mô lớn trong bối cảnh dữ liệu lớn.

1. **Đánh giá rủi ro quyền riêng tư**

Thành phần này đưa ra một đánh giá định tính dựa trên độ nhạy cảm của dữ liệu. Ví dụ, một tổ chức có thể chia các rủi ro thành 5 mức độ và cần có các chiến lược bảo vệ khác nhau. Ngoài ra, việc đánh giá định lượng cũng có thể được đưa ra dựa trên các đánh giá thực nghiệm. Các chỉ số đánh giá có thể được định nghĩa dựa trên các cuộc tấn công quyền riêng tư có thể xảy ra với dữ liệu. Vì dữ liệu của chủ thể dữ liệu có thể được thu thập từ các ứng dụng khác nhau và lưu trữ trên các hệ thống con dữ liệu lớn khác nhau, các rủi ro quyền riêng tư từ việc liên kết các nguồn dữ liệu khác nhau cần được tính đến và đánh giá. Một số kỹ thuật khử định dạng như là quyền riêng tư khác biệt, k-nặc danh, 1-đa dạng,… cung cấp các chỉ số để định lượng rủi ro quyền riêng tư. Các rủi ro quyền riêng tư nên được giám sát liên tục trong suốt vòng đời dữ liệu, đặc biệt là khi dữ liệu được thay đổi hoặc sử dụng trong các bối cảnh khác.

1. **Tính toán bảo toàn quyền riêng tư**

Thành phần này có thể bảo vệ quyền riêng tư của dữ liệu đang được sử dụng. Trên thị trường dữ liệu lớn, các nhà cung cấp dữ liệu có thể muốn kiếm tiền từ dữ liệu mà không phải tiết lộ dữ liệu cho người sử dụng dữ liệu. Ngoài ra, các nhà kiểm soát PII muốn kết hợp dữ liệu của họ cho việc huấn luyện một mô hình máy học. Các công nghệ như là phép giao an toàn, tinh toán đa bên an toàn, mã hóa đồng hình, đồng xử lý bảo mật có thể được sử dụng để hỗ trợ việc tính toán bảo toàn quyền riêng tư.

1. **Giám sát và kiểm soát truy cập**

Thành phần này cung cấp quản lý kiểm soát truy cập và giám sát truy cập cho dữ liệu cá nhân. Việc này có thể phát hiện các truy cập trái phép và phòng ngừa rò rỉ dữ liệu.

1. **Bảo vệ quyền của chủ thể dữ liệu**

Thành phần này kích hoạt các chức năng cần thiết để đảm bảo các quyền của chủ thể dữ liệu. Ví dụ, mô hình quản lý đồng thuận có thể ghi chép lại khi một chủ thể đưa ra/rút lại sự đồng thuận của họ đối với việc thu thập và sử dụng dữ liệu của các ứng dụng. Việc này có thể xóa hoặc ẩn danh dữ liệu một cách an toàn theo các yêu cầu của chủ thể dữ liệu hoặc sau thời gian lưu giữ dữ liệu. Trong một hệ thống dữ liệu lớn, dữ liệu của của cùng một chủ thể dữ liệu có thể được đặt tại các vị trí khác nhau của các ứng dụng khác nhau. Việc kiểm kê dữ liệu có thể giúp trong việc xác định vị trí dữ liệu cá nhân.

## Các chức năng đa lớp cho bảo mật và quyền riêng tư

Các chức năng đa lớp sau đây cho cả bảo mật và quyền riêng tư được nêu rõ trong TCVN ISO/IEC 20547-3:2022 (xem TCVN ISO/IEC 20547-3:2022, Hình 12 và 10.2.6.4):

* khung kiểm toán;
* khung xác thực;
* khung ủy quyền;
* khung ẩn danh.

Như được thể hiện trong Bảng 4, các khung này có thể được hỗ trợ bởi các thành phần chức năng trong 8.2 và 8.3.

Bảng 4 - Các chức năng đa lớp và các thành phần chức năng hỗ trợ cho bảo mật và quyền riêng tư

| **Các chức năng đa lớp** | **Các thành phần chức năng hỗ trợ** |
| --- | --- |
| Khung kiểm toán | 8.2 n) |
| Khung xác thực | 8.2 e), 8.3 j) |
| Khung ủy quyền | 8.2 e), 8.3 b), 8.3 d), 8.3 j), 8.3 k) |
| Khung ẩn danh | 8.3 g) |

# Phụ lục A

# (Tham khảo)

# Các ví dụ về các loại mối đe doạ bảo mật và quyền riêng tư

Bảng A.1 và bảng A.2 liệt kê các mối đe doạ bảo mật và quyền riêng tư. Các mối đe doạ bảo mật tuân thủ theo phân loại STRIDE. Các mối đe doạ quyền riêng tư tuân thủ theo phân loại LINDDUN.

Bảng A.1 - Các loại mối đe doạ bảo mật STRIDE

|  |  |  |
| --- | --- | --- |
| **Mối đe doạ** | **Thuộc tính** | **Mô tả thuộc tính** |
| Giả mạo | Tính xác thực | Danh tính của người dùng được thiết lập (hoặc sẵn sàng chấp nhận người dùng ẩn danh). |
| Xáo trộn | Tính toàn vẹn | Dữ liệu và nguồn lực hệ thống chỉ có thể được thay đổi theo cách thích hợp bới người thích hợp. |
| Chối bỏ | Tính chống chối bỏ | Các người dùng không thể thực hiện một hành động và sau đó từ chối việc thực hiện hành động đó. |
| Tiết lộ thông tin | Tính bí mật | Dữ liệu chỉ sẵn sàng cho những người có dự định truy cập. |
| Từ chối dịch vụ | Tính sẵn sàng | Các hệ thống sẵn sàng khi cần thiết và hoạt động ở mức chấp nhận được. |
| Leo thang đặc quyền | Quyền hạn | Người dùng được cho phép hoặc từ chối một cách rõ ràng việc truy cập vào các tài nguyên. |

Bảng A.2 - Các loại mối đe doạ quyền riêng tư LINDDUN

| **Mối đe doạ** | **Thuộc tính** | **Mô tả thuộc tính** |
| --- | --- | --- |
| Khả năng liên kết | Quyền riêng tư cứng | Tính không liên kết | Ẩn liên kết giữa hai hoặc nhiều các hành vi, danh tính và các mẩu thông tin. |
| Khả năng nhận dạng | Tính ẩn danh | Ẩn liên kết giữa một danh tính và một hành vi hoặc một mẩu thông tin. |
| Khả năng chống chối bỏ | Tính phủ nhận chính đáng | Khả năng phủ nhận đã thực hiện một hành vi, các bên khác không thể xác minh hoặc phủ nhận. |
| Khả năng phát hiện | Tính không thể phát hiện và không thể quan sát | Ẩn các hoạt động của người dùng. |
| Tiết lộ thông tin | Bảo mật | Tính bí mật | Ẩn các nội dung dữ liệu hoặc hoạt động phát hành có kiểm soát nội dung dữ liệu. |
| Không nhận thức | Quyền riêng tư mềm | Nhận thức nội dung | Ý thức của người dùng về dữ liệu của bản thân. |
| Không tuân thủ | Tuân thủ chính sách và thoả thuận | Bộ điều khiển PII thông báo cho chủ thể dữ liệu về chính sách quyền riêng tư của hệ thống hoặc cho phép chủ thể dữ liệu chỉ rõ thoả thuận trong việc tuân thủ luật.  |

# Phụ lục B

# (Tham khảo)

# Các ví dụ về các loại kiểm soát bảo mật và quyền riêng tư

Bảng B.1 liệt kê các loại kiểm soát theo đề xuất trong ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 và ISO/IEC 29151.

Bảng B.1 - Các loại kiểm soát

| **Danh mục** | **Các danh mục con** |
| --- | --- |
| Các chính sách bảo mật thông tin | Định hướng quản lý |
| Tổ chức bảo mật thông tin | Nội bộ tổ chứcCác thiết bị di động và làm việc từ xa |
| Bảo mật nguồn nhân lực | Trước quá trình thực hiện công việcTrong quá trình thực hiện công việc Chấm dứt hoặc chuyển đổi công việc |
| Quản lý tài sản | Trách nhiệm đối với các tài sảnPhân loại thông tin |
| Kiểm soát truy cập | Các yêu cầu nghiệp vụ đối với kiểm soát truy cập Quản lý truy cập người dùngCác trách nhiệm của người dùngKiểm soát truy cập ứng dụng và hệ thống Sử dụng phương tiện truyền thông |
| Mật mã | Các kiểm soát mật mã |
| Bảo mật môi trường và vật lý | Các khu vực bảo mậtThiết bị |
| Bảo mật vận hành  | Các trách nhiệm và quy trình vận hànhBảo vệ khỏi các phần mềm độc hạiSao lưuGiám sát và ghi nhật kýKiểm soát vận hành phần mềmQuản lý lỗ hổng kỹ thuậtCác cân nhắc về kiểm toán các hệ thống thông tin |
| Bảo mật thông tin liên lạc | Quản lý bảo mật mạngChuyền thông tin |
| Tiếp nhận, phát triển và duy trì hệ thống | Các yêu cầu bảo mật cho hệ thống thông tinBảo mật trong các quá trình phát triển và hỗ trợDữ liệu kiểm thử |
| Các quan hệ với nhà cung ứng | Bảo mật thông tin trong các quan hệ với nhà cung ứngQuản lý cung cấp dịch vụ nhà cung ứng |

Bảng B2 và B3 liệt kê các kiểm soát quyền riêng tư khác như được đề xuất trong ISO/IEC 27701, tùy thuộc vào việc tổ chức là bên kiểm soát PII hoặc là bên xử lý PII.

Bảng B.2 - Kiểm soát quyền riêng tư cho các bên kiểm soát PII

| **Danh mục** | **Các biện pháp cho các bên kiểm soát PII** |
| --- | --- |
| Các điều kiện cho việc thu thập và xử lý | Xác định và lưu tài liệu các mục đích |
| Xác định các cơ sở hợp pháp |
| Xác định khi nào và như thế nào để đạt được sự đồng thuận |
| Đạt được và lưu hồ sơ sự đồng thuận |
| Đánh giá tác động quyền riêng tư |
| Các hợp đồng bới các nhà xử lý PII |
| Các hồ sơ liên quân đến xử lý PII |
| Các quyền của chủ PII | Xác định các quyền và khả năng thi hành của các chủ PII |
| Xác định các thông tin cho các chủ PII |
| Cung cấp các thông tin cho các chủ PII |
| Cung cấp cơ chế để sửa đổi và rút lại sự đồng thuận |
| Cung cấp cơ chế để phản đổi việc xử lý |
| Chia sẻ việc thi hành nguyên tắc PII |
| Chỉnh sửa hoặc tẩy xóa |
| Cung cấp cản bản sao PII đã được xử lý |
| Yêu cầu quản lý |
| Ra quyết định tự động |
| Quyền riêng tư mặc định và bám sát thiết kế | Hạn chế thu thập |
| Hạn chế xử lý |
| Định nghĩa và lưu tài liệu các mục tiêu khử nhận dạng và giảm thiểu PII |
| Tuân thủ việc sử dụng khử nhận dạng và giảm thiểu dữ liệu |
| Khửa nhận dạng và xóa bỏ PII |
| Các hồ sợ tàm thời |
| Lưu giữ |
| Loại bỏ |
| Các quy trình thu thập |
| Các kiểm soát truyền PII |
| Chia sẻ, chuyển nhượng và tiết lộ PII | Xác định cơ sở cho chuyển nhượng PII |
| Các quốc gia và tổ chức mà PII có thể được chuyển đến |
| Các hồ sợ chuyển nhượng PII |
| Các hồ sơ tiết lộ PII cho các bên thứ ba |
| Nhà kiểm soát chung |

Bảng B.3 - Kiểm soát quyền riêng tư cho các bên xử lý PII

| **Danh mục** | **Các biện pháp cho các bên xử lý PII** |
| --- | --- |
| Các điều kiện thu thập và xử lý | Thỏa thuận hợp tác |
| Các mục đích của tổ chức |
| Sử dụng tiếp thị và quảng cáo |
| Hướng dẫn vi phạm |
| Các nghĩa vụ của nhà kiểm soát PII |
| Các hồ sơ liên quan đến xử lý PII |
| Các quyền của các chủ PII | Các nghĩa vụ của các chủ PII |
| Hạn chế xử lý |
| Quyền riêng tư mặc định và bám sát thiết kế | Các hồ sơ tạm thời |
| Chuyển trả hoặc loại bỏ PII |
| Các kiểm soát truyền PII |
| Chia sẻ, chuyển nhượng và tiết lộ PII | Cơ sở cho chuyển nhượng PII |
| Các quốc gia và tổ chức mà PII có thể được chuyển đến |
| Các hồ sơ tiết lộ PII cho các bên thứ ba |
| Thông báo các yêu cầu tiết lộ PII |
| Các tiết lộ ràng buộc pháp lý |
| Tiết lộ các nhà thầu phụ được dùng để xử lý PII |
| Sự tham gia của một nhà thầu phụ để xử lý PII |
| Sự thay đổi nhà thầu phụ để xử lý PII |

# Phụ lục C

# (Tham khảo)

# Các ví dụ về hệ sinh thái và kết quả điều phối các hoạt động bảo mật và quyền riêng tư

**C.1. Ánh xạ các tổ chức của hệ sinh thái tới BDRA**

Ví dụ này được phỏng theo dự án nghiên cứu dữ liệu lớn công nghệ ô tô AutoMat. Mục dích của ví dụ nay là để đưa ra các ví dụ cụ thể về cách mà hệ sinh thái được điều phối. Hệ sinh thái liên quan đến các tổ chức sau (xem Hình C.1):

* Các nhà sản xuất công nghệ ô tô đóng vai trò BDRA là nhà cung cấp dữ liệu lớn, và các vai trò phụ là nhà cung cấp thu thập dữ liệu lớn và cung cấp chuẩn bị dữ liệu lớn. Họ cài đặt một hệ thống thu thập dữ liệu có sự đồng ý của các chủ sơ hữu phương tiện, thu thập dữ liệu và chuẩn bị chúng dưới một dạng định dạng tương thích (mô hình thông tin phương tiên phổ biến);
* Các nhà cung cấp kho lưu trữ đóng vai trò BDRA phụ là nhà cung cấp cơ sở hạ tầng dữ liệu lớn. Họ quản lý dữ liệu ở trạng thái nghỉ. Dữ liệu được thu thập được lưu trữ và quản lý riêng trong các tài khoản của các chủ sở hữu phương tiện;

Các thị trường đóng vai trò phụ BDRA là nhà cung cấp nền tảng dữ liệu lớn và nhà cung cấp xử lý dữ liệu lớn. Dữ liệu được thu thập từ các nhà cung cấp kho lưu trữ và biến đổi chúng thành các tập dữ liệu có thể sử dụng được bởi các nhà cung cấp dịch vụ; và

* Các nhà cung cấp dịch vụ đóng các vai trò phụ BDRA là nhà cung cấp phân tích dữ liệu lớn, nhà cung cấp trực quan hóa dữ liệu lớn, nhà cung cập truy cập dữ liệu lớn và vai trò BDRA là người dùng dữ liệu lớn.

Những điều sau đây có thể được quan sát:

* Việc ánh xạ giữa các vai trò và các tổ chức không phải là 1-1;
* Khách hàng của nhà cung cấp kho lưu trữ là các chủ phương tiện trực tiếp kiểm soát việc sử dụng dữ liệu; và
* Thị trường dựa trên các tập dữ liệu nhanh do các nhà cung cấp dịch vụ yêu cầu.



Hình C.1 - Ví dụ hệ sinh thái theo BDRA

**C.2. Điều phối hệ sinh thái**

Hệ sinh thái tuân theo cách tiếp cận hệ sinh thái dữ liệu cá nhân. Trong khi các nhà sản công nghệ ô tô là một phần của hệ sinh thái khi họ đóng vai trò là nhà cung cấp dữ liệu lớn và các vai trò phụ là nhà cung cấp thu thập dữ liệu lớn và nhà cung cấp chuẩn bị dữ liệu lớn, họ lại không trực tiếp liên quan đến việc trao đổi dữ liệu lớn với các nhà cung cấp dịch vụ. Việc này được quản lý bởi thị trường đóng vai trò như là người môi giới giữa các chủ phương tiện và các nhà cung cấp dịch vụ. Hình C.2 thể hiện hai đặc điểm kết quả của hệ sinh thái;

* Dữ liệu được lưu trữ theo các tài khoản của phương tiện;
* Một mô tả tương thích được cung cấp cho thị trường (được gọi là mô hình thông tin phương tiện phổ biến hoặc CVIM).



Hình C.2 - Hệ sinh thái dữ liệu cá nhân AutoMat

Các nhu cầu phối hợp kết quả là như sau:

* Một kế hoạch tiếp cận đồng thuận cần phải được đưa ra để định nghĩa cho mô hình thông tin phương tiện chung; và
* Các năng lực bảo mật và quyền riêng tư của các nhà sản xuất công nghệ ô tô, của các nhà quản lý kho lưu trữ, của các thị trường và của các nhà cung cấp dịch vụ phụ thuộc lẫn nhau. Đặc biệt, họ cần có các hoạt động bảo mật và quyền riêng tư nhất quán như sau:
	+ đối với phân tích mối nguy;
	+ đối với phân tích rủi ro; và
	+ đối với thiết kế kiểm soát.

**C.3. Phối hợp các mối đe doạ bảo mật và quyền riêng tư giữa thị trường và nhà cung cấp dịch vụ**

Bảng C.1 thể hiện các mối đe doạ bảo mật và quyền riêng tư điển hình cho tổ chức thị trường.

Bảng C.1 - Các mối đe doạ cho các tổ chức thị trường

|  |
| --- |
| **Các mối đe doạ bảo mật** |
| Giả mạo | Giả mạo nhà cung cấp lưu trữ đám mây hoặc nhà cung cấp dịch vụ. |
| Xáo trộn | Sự toàn vẹn và đầy đủ của dữ liệu (để tránh việc cung cấp dữ liệu bị hư hỏng và tổn hại cho các nhà cung cấp dịch vụ). |
| Chối bỏ | Nhà quản lý dịch vụ cung cấp sự chống chối bỏ (dịch vụ đưa ra lời đề nghị mà sau đó từ chối việc đưa ra lời đề nghị đó). |
| Tiết lộ thông tin | Nghe trộm dữ liệu trong quá trình liên lạc.Nghe trộm siêu dữ liệu (ví dụ: nhật ký các tương tác với thị trường).Việc quản lý đường ống dữ liệu không đúng cách dẫn tới rò rỉ (ví dụ: xóa bỏ không chính xác). |
| Từ chối dịch vụ | Lượng lớn truy cập vào thị trường bởi các nhà cung cấp dịch vụ giả mạo. |
| Leo thang đặc quyền | Quản lý các luật quyền riêng tư chủ sở hữu phương tiên không đùng cách. |
| **Các mối đe doạ quyền riêng tư** |
| Tính liên kết | Việc ẩn danh không được thực hiện đúng cáchCác mối đe doạ tính liên kết không được tính đến trong vòng đời (ví dụ: việc xác định một người trong một hệ thống đùng về mặt pháp luật). |

Bảng C.2 thể hiện các mối đe doạ bảo mật và quyền riêng tư điển hình đối với tổ chức nhà cung cấp dịch vụ.

Bảng C.2 - Các mối đe doạ cho tổ chức các nhà cung cấp dịch vụ

|  |
| --- |
| **Các mối đe doạ bảo mật** |
| Giả mạo | Giả mạo thị trường |
| Xáo trộn | Sự toàn vẹn và đầy đủ của dữ liệu (để tránh việc cung cấp dữ liệu bị hư hỏng và tổn hại cho các nhà cung cấp dịch vụ). |
|  **Tính chống khoái thác**  |
| Tiết lộ thông tin | Nghe trộm dữ liệu trong quá trình liên lạc.Nghe trộm siêu dữ liệu (ví dụ: nhật ký các tương tác với backend OEM, nhật ký các tương tác với thị trường).Quản lý các chuỗi xử lý dữ liệu không đúng cách dẫn đến rò rỉ (ví dụ: xóa bỏ không chính xác). |
| Từ chối dịch vụ | Lượng lớn truy cập vào thị trường  |
| **Các mối đe doạ quyền riêng tư** |
| Tính liên kết | Việc ẩn danh không được thực hiện một cách chính xác.Nỗ lực từ các nhóm bên ngoài nhằm xác định lại chủ sở hữu phương tiện bằng cách sử dụng các tập dữ liệu khác.Mối đe dọa khả năng liên kết không được tính đến trong vòng đời. |

**C.4. Phối hợp các rủi ro giữa thị trường và nhà cung cấp dịch vụ**

Bảng C.3 liệt kê các vi phạm cần xem xét đối với một tổ chức thị trường.

Bảng C.3 - Các vi phạm cho các tổ chức thị trường

| **Vi phạm** | **Mô tả vi phạm** | **Tác động chung** |
| --- | --- | --- |
| Trường hợp vi phạm dữ liệu cá nhân | Báo cáo không khai rằng kho dữ liệu cá nhận bị truy cập hoặc đã được xử lý mà không có sự đồng ý hoặc đi ngược các luật quyền riêng tư. | Đáng kể. |
| Rò rỉ dữ liệu kinh doanh hàng loạt | Báo cáo công khai khả năng rò rỉ dữ liệu kinh doanh hàng loạt bởi hoạt động không thích hợp ở cấp thị trường. | Tối đa. |
| Vi phạm dữ liệu cá nhân hàng loạt | Báo cáo công khai khả năng rò rỉ dữ liệu cá nhân hàng loạt bởi hoạt động không thích hợp ở cấp thị trường. | Tối đa. |
| Từ chối dịch vụ hàng loạt | Thị trường không thể hoạt động được nữa. | Đáng kể. |

Bảng C.4 liệt kê các vi phạm điển hình cần xem xét đối với một tổ chức nhà cung cấp dịch vụ.

Bảng C.4 - Các vi phạm cho các tổ chức nhà cung cấp dịch vụ

|  |  |  |
| --- | --- | --- |
| **Vi phạm** | **Mô tả vi phạm** | **Tác động chung** |
| Vi phạm dữ liệu cá nhân hàng loạt | Báo cáo công khai khả năng rò rỉ dữ liệu cá nhân hàng loạt bởi hoạt động không thích hợp ở cấp nhà cung cấp dịch vụ. | Tối đa. |
| Từ chối dịch vụ hàng loạt | Nhà cung cấp dịch vụ không thể hoạt động được nữa. | Đáng kể. |

**C.5. Phối hợp các kiểm soát giữa thị trường và nhà cung cấp dịch vụ**

Bảng C.5 liệt kê các biện pháp đã được xác định để xử lý các mối đe doạ được xác định của một thị trường.

Bảng C.5 - Các kiểm soát trong tổ chức thị trường

| **Danh mục** | **Danh mục con** | **Kiểm soát** | **Mô tả** |
| --- | --- | --- | --- |
| Các chính sách bảo mật thông tin | Định hướng quản lý | Các chinh sách quản lý dữ liệu | Tích hợp các chính sách quản lý dữ liệu nghiệp vụ (truy cập kiểm soát, bảo vê, minh bạch, các thỏa thuận nghiệm vụ) bao gồm cả chủ sở hữu phương tiện (các luật quyền riêng tư). |
| An ninh nguồn nhân lực | Trong quá trình công tác | Sự sẵn sàng an ninh mạng nội bộ | Đào tạo và sẵn sàng đối với các cuộc tấn công an ninh mạng trên thị trường. |
| Sự sẵn sàng an ninh mạng bên ngoài | Đào tạo và sẵn sàng đối với các cuộc tấn công an ning mạng trong tổng thể quá trình xử lý chuỗi dữ liệu AutoMat. Điều này liên quan đến các đào tạo chung với các bên liên quan thành phần khác (OEM, nhà cung cấp lưu trữ đám mây, nhà cung cấp dịch vụ) |
| Truy cập kiểm soát | Các yêu cầu nghiệp vụ đối với truy cập kiểm soát | Các yêu cầu đối với quyền truy cập nhà cung cấp dịch vụ | Tích hợp các yêu cầu để cho phép nhà cung cấp dịch vụ đưa ra yêu cầu cung cấp thông tin phương tiện. |
| Truy cập kiểm soát ứng dụng và hệ thống | Truy cập an toàn từ nhà cung cấp dịch vụ | Hỗ trợ kết nối được xác thực giữa nhà cung cấp dịch vụ và thị trường. |
| Truy câp an toàn tới nhà cung cấp lưu trữ đám mây | Hỗ trợ kết nối được xác thực giữa thị trường và nhà cung cấp lưu trữ đám mây. |
| Mật mã | Các kiểm soát mật mã | Tính bí mật của kho dữ liệu cá nhân | Truy cập được mã hóa tới nhà cung cấp lưu trữ đám mây. |
| Ẩn danh các tập dữ liệu | Che dấu dữ liệu các tập dữ liệu. |
| Bảo mật hoạt động | Các trách nghiệm và quy trình vận hành | Các quy trình vận hành xư lý và tìm kiếm dữ liệu | Tích hợp đường ống dữ liệu an toàn và tìm kiếm an toàn. |
| Giám sát và ghi nhật ký | Khả năng ghi nhật ký | Nhật ký an toàn các hành động động cho bảo mật và quyền riêng tư. |
| Kiểm soát phần mềm vận hành | Các quy trình vận hành nhằm mình bạch | Tích hợp các hoạt động quản lý minh bạch. |
| Bảo mật thông tin liên lạc  | Chuyển giao thông tin | Truyền dữ liệu an toàn | Truyền dữ liệu an toàn giữa nhà cung cấp lưu trữ đám mây và trị trường và giữa thị trường và nhà cung cấp dịch vụ. |
| Tiếp nhận, phát triển và duy trì hệ thống | Bảo mật trong các quy trình hỗ trợ và phát triển | Năng lực bảo mật đường ống dữ liệu  | Thiết kế các năng lực bảo mật trên thị trường để quản lý đường ống dữ liệu một cách an toàn. |
| Năng lực giám sát an ninh mạng | Tích hợp trung tâm vận hành bảo mật thị trường trong các hoạt động thị trường. |
| Quản lý các sự cố bảo mật thông tin | Quản lý các sự cố và cải tiến bảo mật thông tin | Cảnh báo chuỗi xử lý dữ liệu | Cảnh báo chuỗi xử lý dữ liệu trong trường hợp có sự cố an ninh mạng. Trong trường hợp một vấn đề gây nguy hiểm đến đặc tả mô hình thông tin chung, cảnh báo các nhóm tiêu chuẩn hóa CVIM. |
| Các khía cạnh bảo mật thông tin của quản lý nghiệp vụ liên tục | Bảo mật thông tin liên tục | Sự đảm bảo năng lực an ninh mạng của nhà quản lý lưu trữ đám mây | Đảm bảo thường xuyên năng lực ghi nhật ký của thị trường. |
| Xem xét định ký năng lực an ninh mạng của nhà quản lý lưu trữ đám mây | Phân tích định kỳ rủi ro bảo mật và quyền riêng tư ở phía thị trường. |
| Tuân thủ | Tuân thủ các yêu cầu pháp lý và hợp đồng | Xác minh sự tuân thủ GDPR và an ninh mạng | Thể hiện rằng chuối xử lý dữ liệu thị trường tuân thủ với quy định GDPR cũng như với Luật An ninh mạng trong tương lai. |
| Các xem xét bảo mật thông tin | Xem xét định kỳ khả năng tương thích | Xem xét định kỳ đặc tả khả năng tương thích CVIM về mặt tuân thủ bảo mật và quyền riêng tư. |

Bảng C.6 liệt kê các biện pháp đã được xác định để xử lý các rủi ro các được xác định của một nhà cung cấp dịch vụ.

Bảng C.6 - Các kiểm soát cho tổ chức nhà cung cấp dịch vụ

| **Danh mục** | **Danh mục con** | **Kiểm soát** | **Mô tả** |
| --- | --- | --- | --- |
| Các chính sách bảo mật thông tin | Định hướng quản lý | Các chính sách quản lý dữ liệu | Tích hợp các chính sách quản lý dữ liệu nghiệp vụ (truy cập kiểm soát, bảo vệ, minh bạch, các thỏa thuận nghiệp vụ). |
| Bảo mật nguồn nhân lực | Trong quá trình công tác | Sự sẵn sàng an ninh mạng nội bộ | Đào tạo và sẵn sàng đối với các cuộc tấn công an ninh mạng trên thị trường |
| Sự sẵn sàng an ninh mạng bên ngoài | Đào tạo và sẵn sàng đối với các cuộc tấn công an ninh mạng trong tổng thể quá trình xử lý chuỗi dữ liệu AutoMat. Điều này liên quan đến các đào tạo chung với các bên liên quan thành phần khác (OEM, nhà cung cấp lưu trữ đám mây, nhà cung cấp dịch vụ). |
| Truy cập kiểm soát | Truy cập kiểm soát ứng dụng và hệ thống | Truy cập an toàn tới nhà cung cấp thị trường | Hỗ trợ kết nối được xác thực giữa nhà cung cấp dịch vụ và thị trường. |
| Mật mã | Các kiểm soát mật mã | Ẩn danh các tập dữ liệu | Che dấu dữ liệu các tập dữ liệu. |
| Bảo mật hoạt động | Các trách nghiệm và quy trình vận hành | Các quy trình vận hành xử lý dữ liệu | Liên kết của xử lý dữ liệu bảo mật. |
| Giám sát và ghi nhật ký | Khả năng ghi nhật ký | Nhật ký bảo mật của các hành vi cho bảo mật và quyền riêng tư. |
| Kiểm soát phần mềm vận hành | Các quy trình vận hành nhằm mình bạch | Liên kết các hoạt động quản lý minh bạch. |
| Quản lý lỗ hổng kỹ thuật | Kiểm tra tính hợp lý | Đảm bảo rằng dữ liệu được cung cấp không bị giả mạo thông qua một số ứng dụng. |
| Bảo mật thông tin liên lạc  | Chuyển giao thông tin | Truyền dữ liệu an toàn | Truyên dữ liệu an toàn giữa thị trường và nhà cung cấp dịch vụ. |
| Tiếp nhận, phát triển và duy trì hệ thống | Bảo mật trong các quy trình hỗ trợ và phát triển | Năng lực xư lý dữ liệu an toàn | Thiết kế năng lực bảo mật trong nhà cung cấp dịch vụ để quản lý xử lý dữ liệu một cách an toàn. |
| Năng lực giám sát an ninh mạng | TÍch hợp năng lực giám sát an ninh mạng trong các hoạt động của nhà cung cấp dịch vụ. |
| Quản lý sự cố bảo mật thông tin | Quản lý các sự cố và cải tiến bảo mật thông tin | Cảnh báo chuỗi xư lý dữ liệu | Cảnh báo chuỗi xư lý dữ liệu trong trường hợp có sự cố an ninh mạng. Trong trường hợp một vấn đề gây nguy hiểm đến đặc tả mô hình thông tin chung, cảnh báo các nhóm tiêu chuẩn hóa CVIM. |
| Các khía cạnh bảo mật thông tin của quản lý nghiệp vụ liên tục | Bảo mật thông tin liên tục | Sự đảm bảo năng lực an ninh mạng của nhà cung cấp dịch vụ | Sự đảm bảo thường xuyên năng lực ghi nhật ký an toàn trong thành phần nhà cung cấp dịch vụ. |
| Xem xét định kỳ năng lực an ninh mạng của nhà cung cấp dịch vụ | Phân tích định kỳ rủi ro bảo mật và quyền riêng tử ở phía nhà cung cấp dịch vụ. |
| Tuân thủ | Tuân thủ các yêu cầu pháp lý và hợp đồng | Xác minh sự tuân thủ GDPR và an ninh mạng | Thể hiện rằng chuối xử lý dữ liệu thị trường tuân thủ với quy định GDPR cũng như với Luật An ninh mạng trong tương lai. |
| Các xem xét bảo mật thông tin | Xem xét định kỳ khả năng tương thích | Xem xét định kỳ đặc tả khả năng tương thích CVIM về mặt tuân thủ bảo mật và quyền riêng tư. |

# Phụ lục D

# (Tham khảo)

# Ví dụ về kiểm soát bảo mật và quyền riêng tư cho mỗi vai trò BDRA

**D.1. Các ví dụ về các kiểm soát bảo mật và quyền riêng tư cho nhà cung cấp ứng dụng dữ liệu lớn (BDAP)**

Bảng D.1 liệt các các kiểm soát bảo mật và quyền riêng tư cho nhà cung cấp ứng dụng dữ liệu lớn (BDAP).

Bảng D.1 - Các kiểm soát bảo mật và quyền riêng tư cho BDAP

| **Danh mục** | **Danh mục con** | **Ví dụ về các kiểm soát BDAP** | **Mô tả** |
| --- | --- | --- | --- |
| Các chính sách bảo mật thông tin | Định hướng quản lý | Các chính sách quản lý dữ liệu | Tích hợp các chính sách quản lý cung cấp dữ liệu cụ thể (bảo vệ tổ chức, minh bạch, các thỏa thuận nghiệp vụ)Tích hợp các chính sách PII (sự đồng ý, tinh ẩn danh) nếu như dữ liệu thu thập có bao gồm PII. ISO/IEC 27701 cung cấp một danh sách các biện pháp quyền riêng tư. |
| Tổ chức bảo mật thông tin | Tổ chức nội bộ |  |  |
| Các thiết bị di động và làm việc từ xa |  |  |
| Bảo mật nguồn nhân lực | Trước quá trình công tác |  |  |
| Trong quá trình công tác | Sự sẵn sàng đối với an ninh mạng nội bộ  | Đào tạo và sẵn sàng chống lại các vi phạm an ninh mạng trong các hoạt động liên quan đến cung cấp dữ liệu. |
| Sự sẵn sàng đối với an ninh mạng bên ngoài | Đào tạo và sẵn sàng chống lại các vi phạm an ninh mạng trong hệ sinh thái dữ liệu lớn tổng thể. Điều này liên quan đến các đào tạo chung với các bên liên quan khác trong các vai trò khác (BDSP, BDP, BDFP, BDC). |
| Kết thúc hoặc thay đổi công tác |  |  |
| Quản lý tài sản | Trách nhiệm đối với các tài sản |  |  |
| Phân loại thông tin |  |  |
| Kiểm soát truy cập | Các yêu cầu nghiệp vụ đối với kiểm soát truy cập  | Các yêu cầu kiểm soát truy cập đối với dữ liệu được thu thập | Liên kết các yêu cầu kiểm soát truy cập cho chuỗi xử lý dữ liệu trong BDAP. |
| Quản lý truy cập người dùng |  |  |
| Các trách nhiệm người dùng |  |  |
| Kiểm soát truy cập ứng dụng và hệ thống | Truy cập an toàn vào dữ liệu và siêu dữ liệu do BDP quản lý | Hỗ trợ kết nối có xác thực giữa BDAP và các bên liên quan. |
| Truyền thông |  |  |
| Mật mã | Các kiểm soát mật mã | Tính bí mậtt và khử nhận dạng của dữ liệu được thu thập | Áp dụng các kỹ thuật khử nhận dạng cho dữ liệu khi cần thiết.ISO/IEC 20889 cung cấp một danh mục con các yêu cầu kỹ thuật tương tự.Bảo mật dữ liệu ở trạng thái nghỉ. Các chính sách truy cập dữ liệu dựa trên các thông tin đăng nhập.Bảo mật PII. PII, ví dụ như là dữ liệu người dùng nhạy cảm, được mã hõa |
| Bảo mật môi trường và vật lý | Các khu vực bảo mật |  |  |
| Thiết bị |  |  |
| Bảo mật hoạt động  | Các trách nhiệm và quy trình vận hành | Các quy trình vận hành để có sự đồng thuận về các vai trò khác nhau của BDAP: thu thập, chuẩn bị, cung cấp các phân tích, trực quan hóa và cung cấp dữ liệu.  | Tích hợp chuỗi xử lý an toàn vào các vai trò con khác nhau của BDAP. Điều này bao gồm việc thực thi chính sách.Các ví dụ về các cơ chế như là các danh sách kiểm soát truy cập (ACLs) và các ranh giới máy ảo hóa (VM).Tích hợp các hoạt động quản lý sự đồng ý trong trường hợp PII. |
| Bảo vệ khỏi phần mềm độc hại |  |  |
| Sao lưu |  |  |
| Giám sát và ghi nhật ký | Các năng lực ghi nhật ký | Ghi nhật ký an toàn các hành động BDAP đối với bảo mật và quyền riêng tư. |
| Kiểm soát phần mềm vận hành | Quy trình vận hành nhằm minh bạch | Tích hợp các hoạt động quản lý minh bạch. |
| Quản lý lỗ hổng kỹ thuật |  |  |
| Các cân nhắc về kiểm toán hệ thống thông tin |  |  |
| Bảo mật thông tin liên lạc | Quản lý bảo mật mạng |  |  |
| Chuyển giao thông tin | Truyền dữ liệu an toàn | Truyền dữ liệu an toàn trong các vai trò con khác nhau của BDAP. Bảo mật dữ liệu trong qua trình chuyển tiếp. Ví dụ, được thực thi bằng việc sử dụng bảo mật lớp truyền tải (TLS). |
| Tiếp nhận, phát triển và duy trì hệ thống | Các yêu cầu bảo mật của hệ thống thông tin |  |  |
| Bảo mật trong các quá trình phát triển và hỗ trợ | Tính toàn vẹn của quá trình thu thập PII | Thiết kế các năng lực cho BDAP để đảm bảo tính toàn vẹn của quá trình thu thập PII liên quan đến các chính sách và sự đồng thuận. |
| Kho lưu trữ quản lý sự đồng thuận | Thiết kế các năng lực quản lý sự đồng thuận của BDAP. Điều này bao gồm hỗ trợ quan hệ chủ PII. |
| Các năng lức giám sát an ninh mạng | Tích hợp năng lực giám sát xử lý chuỗi dữ liệu trong các hoạt động BDAP. |
| Dữ liệu kiểm thử |  |  |
| Các mối quan hệ với các nhà cung cấp | Bảo mật thông tin trong các mối quan hệ với nhà cung cấp |  |  |
| Quản lý phân phối dịch vụ nhà cung cấp |  |  |
| Quản lý sự cố bảo mật thông tin | Quản lý các sự cố và cải tiến bảo mật thông tin | Cảnh bảo hệ sinh thái | Cảnh báo hệ sinh thái trong trường hợp sự cố an ninh mạng có thể gây nguy hiểm cho tính toàn vẹn dữ liệu. |
| Các khía cảnh bảo mật thông tin của quản lý kinh doanh liên tục | Bảo mật thông tin liên tục | Đảm bảo năng lực an ninh mạng của BPD | Đảm bảo thường xuyên các biện pháp kiểm soát được thực hiện trong các hoạt động BDAP. |
| Đánh giá định kỳ năng lực an nình mạng của BDP | Phân tích định kỳ các rủi ro bảo mật và quyền riêng tư trong các hoạt động BDAP. |
| Các dư thừa |  |  |
| Sự tuân thủ | Sự tuân thủ các yêu cầu pháp lý và hợp đồng | Xác minh sự tuân thủ bảo mật và quyền riêng tư | Chứng minh rằng các hoạt động BDAP tuân thủ với các yêu cầu pháp lý và hợp đồng. |
| Các đánh giá bảo mật thông tin | Đánh giá định kỳ khả năng tương tác | Đánh giá định kỳ đặc tả khả năng tương tác về mặt tuân thủ bảo mật và quyền riêng tư. |
| Kiểm soát quyền riêng tư | Các điều kiện thu thập và xử lý  |  | Áp dụng các biện pháp nếu như BDAP bao gồm các trách nhiệm điều khiển dữ liệu hoặc xử lý dữ liệu (xem ISO/IEC 27701). |
| Quyển của các chủ PII |  |
| Quyền riêng tư theo thiết kế và theo mặc định |  |
| Chia sẻ, chuyển nhượng và tiết lộ PII |  |

**D.2. Các ví dụ về các kiểm soát bảo mật và quyền riêng tư cho nhà cung cấp dữ liệu lớn (BDP)**

Bảng D.2 liệt kê các kiểm soát bảo mật và quyền riêng tư đã được phân loại cho nhà cung cấp dữ liệu lớn (BDP).

Bảng D.2 - Các kiểm soát bảo mật và quyền riêng tư cho BDP

| **Danh mục** | **Danh mục con** | **Ví dụ về các kiểm soát BDP** | **Mô tả** |
| --- | --- | --- | --- |
| Các chính sách bảo mật thông tin | Chỉ đạo quản lý | Các chính sách quản lý dữ liệu  | Tích hợp các chính sách quản lý cung cấp dữ liệu cụ thể (bảo vệ tổ chức, minh bạch, thỏa thuận kinh doanh)Tích hợp các chính sách PII cụ thể (sự đồng ý, sự ẩn danh) nếu như dữ liệu thu thập bao gồm PII. ISO/IEC 27701 cung cấp một danh sách các biện pháp quyền riêng tư. |
| Tổ chức bảo mật thông tin | Tổ chức nội bộ |  |  |
| Thiết bị di động và làm việc từ xa |  |  |
| Bảo mật nguồn nhân lực | Trước khi tuyển dụng |  |  |
| Trong quá trình công tác | Chuẩn bị sẵn sàng cho an ninh mạng nội bộ | Đào tạo và chuẩn bị sẵn sàng chống lại các vi phạm an ninh mạng trong các hoạt động liên quan đến cung cấp dữ liệu. |
| Chuẩn bị sẵn sàng cho an ninh mạng từ bên ngoài | Đào tạo và chuẩn bị sẵn sàng chống lịa các vị phạm an ninh mạng trong tổng thể hệ sinh thái dữ liệu lớn. Điều này liên quan đến việc đào tạo chung với các bên liên quan khác trong các vai trò khác (BOSP, BDAP, BDFP, BDC). |
| Chấm dứt hoặc thai đổi công tác |  |  |
| Quản lý tài sản | Trách nhiệm đối với các tài sản |  |  |
| Phân loại thông tin |  |  |
| Kiểm soát truy cập | Các yêu cầu nghiệp vụ cho kiểm soát truy cập | Các yêu cầu kiểm soát truy cập đối với dữ liệu thu thập | Tich hợp các yêu cầu kiểm soát truy cập cho chuỗi xử lý dữ liệu trong BDAP. |
| Quản lý truy cập người dùng |  |  |
| Các trách nhiệm của người dùng |  |  |
| Kiểm soát truy cập ứng dụng và hệ thống | Truy cập an toàn vào dữ liệu và siêu dữ liệu quản lý bởi BDP | Hỗ trợ kết nối được xác thực giữa BDP và các bên liên quan khác. |
| Phương tiện truyền thông |  |  |
| Mật mã | Kiểm soát mật mã | Tính bảo mật và khử nhận dạng của dữ liệu thu thập | Áp dụng các kỹ thuật khử nhận dạng cho dữ liệu khi cần thiết.ISO/IEC 20889 cung cấp danh mục con các yêu cầu kỹ thuật tương tự. |
| Bảo mật môi trường và vật lý | Khu vực an ninh |  |  |
| Thiết bị |  |  |
| Bảo mật vận hành | Các trách nhiệm và quy trình vận hành | Các quy trình vận hành đối cho sự đồng thuận việc mở và phân phối nguồn dữ liệu | Tich hợp chuối xử lý an toàn trong việc mở và phân phối nguồn dữ liệu.Tích hợp các hoạt động quản lý sự đồng thuận đối trong trường hợp PII. |
| Bảo vệ khỏi phần mềm đọc hại |  |  |
| Sao lưu |  |  |
| Giám sát và ghi nhật ký | Các năng lực ghi nhật ký | Ghi nhật ký an toàn các hành động của BDP đối với bảo mật và quyền riêng tư. |
| Kiểm soát phần mềm vận hành | Các quy trình vận hành minh bạch | Tích hợp các hoạt động quản lý tính minh bạch. |
| Quản lý lỗ hổng kỹ thuật |  |  |
| Các cân nhắc kiểm toán các hệ thống thông tin |  |  |
| Bảo mật truyền thông | Quản lý an ninh mạng |  |  |
| Trao đổi thông tin | Truyền dữ liệu an toàn | Truyền dữ liệu an toàn từ nguồn tới đích. |
| Tiếp nhận, phát triển và duy trì hệ thống | Các yêu cầu bảo mật của hệ thống thông tin |  |  |
| Bảo mật trong quá trình phát triển và hỗ trợ | Tích hợp quá trình thu thập PII | Thiết kế các khả năng cho BDP để đảm bảo tính toàn vẹn của quá trình thu thập PII liên quan đến các chính sách và sự đồng thuận. |
| Kho quản lý sự đồng thuận | Thiết kế các khả năng cho quản lý sự đồng thuận của BDP. Điều này bao gồm hỗ trợ quan hệ chủ PII. |
| Các năng lực giám sát an ninh mạng | Tích hợp năng lực giám sát xử lý chuỗi dữ liệu trong các hoạt động BDP. |
| Dữ liệu kiểm tra |  |  |
| Các mối quan hệ với các nhà cung cấp | Bảo mật thông tin trong các mối quan hệ nhà cung cấp |  |  |
| Quản lý phân phối dịch vụ nhà cung cấp |  |  |
| Quản lý sự cố bảo mật thông tin | Quản lý các sự cố và cải tiến bảo mật thông tin | Cảnh báo hệ sinh thái | Cảnh báo hệ sinh thái trong trường hợp sự cố an ninh mạng có thể gây nguy hiểm tới tính toàn vẹn của dữ liệu. |
| Các khía cảnh bảo mật thông tin của quản lý nghiệp vụ liên tục | Tính liên tục của bảo mật thông tin | Đảm bảo năng lực an ninh mạng của BPD | Đảm bảo thường xuyên thực hiện các biện pháp kiêm soát trong các hoạt động của BDP. |
| Đánh giá định kỳ năng lực an ninh mạng của BPD | Phân tích định kỳ rủi ro bảo mật và quyền riêng tư trong các hoạt động BPD. |
| Các dư thừa |  |  |
| Sự tuân thủ | Tuân thủ với các yêu cầu hợp đồng và pháp luật  | Xác minh sự tuân thủ bảo mật và quyền riêng tư | Thể hiện các hoạt động BDAP tuân thủ với các yêu cầu hợp đồng và pháp luật. |
| Các đánh giá bảo mật thông tin | Đánh giá định kỳ tính tương tác | Đánh giá định kỳ tính đặc tả tính tương tác về mặt tuân thủ bảo mật và quyền riêng tư. |
| Các kiểm soát quyền riêng tư | Các điều kiện đối với việc thu thập và xử lý |  | Áp dụng các biện pháp nếu như BDP bao gồm cả các trách nhiệm điều khiển dữ liệu hoặc xử lý dữ liệu (xem ISO/IEC 27701). |
| Các quyền của chủ PII |  |
| Quyền riêng tư theo thiết kế và theo mặc định |  |
| Chia sẻ, chuyển nhượng và tiết lộ PII |  |

# Thư mục tài liệu tham khảo

1. TCVN ISO/IEC TR 20547-1:2022 (ISO/IEC TR 20547-1:2020): Công nghệ thông tin - Kiến trúc tham chiếu dữ liệu lớn - Phần 1: Khung và quy trình ứng dụng.
2. TCVN 13239-2:2020 (ISO/IEC TR 20547-2:2018): Công nghệ thông tin - Kiến trúc tham chiếu dữ liệu lớn - Phần 2: Các trường hợp sử dụng và yêu cầu dẫn xuất.
3. TCVN 13239-5:2020 (ISO/IEC TR 20547-5:2018): Công nghệ thông tin - Kiến trúc tham chiếu dữ liệu lớn - Phần 5: Lộ trình tiêu chuẩn.
4. ISO/IEC 20889, Privacy enhancing data de-identification terminology and classification of techniques.
5. ISO/IEC 21827, Information technology - Security techniques - Systems Security Engineering — Capability Maturity Models (SSE-CMM@).
6. ISO/IEC 24760, IT Security and Privacy - A framework for identity management.
7. ISO/IEC 24760-3, Information technology - Security techniques - A framework for identity management - Part 3: Practice.
8. ISO/IEC 27000, Information technology - Security techniques - Information security management systems - Overview and vocabulary.
9. ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements.
10. ISO/IEC 27002, Information technology - Security techniques - Code of practice for information securit y controls.
11. ISO/IEC 27005, Information technology - Security techniques - Information security risk management.
12. ISO/IEC 27009, Information security, cybersecurity and privacy protection - Sector-specific application of ISO/IEC 27001 – Requirements.
13. ISO/IEC TR 27550, Information technology - Security techniques - Privacy engineering for system life cycle processes.
14. ISO/IEC 27701, Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines.
15. ISO/IEC 29100, Information technology - Securit y techniques - Privacy framework
16. ISO/IEC 29134. Information technology - Security techniques - Guidelines for privacy impact assessment.
17. ISO/IEC 29146, Information technology - Security techniques - A framework for access management.
18. ISO/IEC 29151, Information technology - Security techniques - Code of practice for personally identifiable information protection.
19. IS0/IEC /IEEE 42020, Software, systems and enterprise - Architecture processes.
20. NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations.
21. NIST SP 1500-4, NIST Big Data Interoperability Framework: Volume 4, Securit y and Privacy, Version 2, June 2018.
22. The STRIDE threat model, available at: httns' //msdn microsoft com/en-us/librarv/ ee823878fv=cs 20) asnx.
23. LINDDUN privacy threat analysis methodology, available at: httns'//www linddun.org/.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_