TRƯỜNG ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN - VNUHCM - UIT

QUẢN LÝ RỦI RO AN TOÀN THÔNG TIN TRONG DOANH NGHIỆP

Chương 1
Giới thiệu về QLRR - Phạm vi QLRR – Các thuật ngữ và định nghĩa

Nội dung

01

- GIỚI THIỆU VỀ QUẢN LÝ RỦI RO

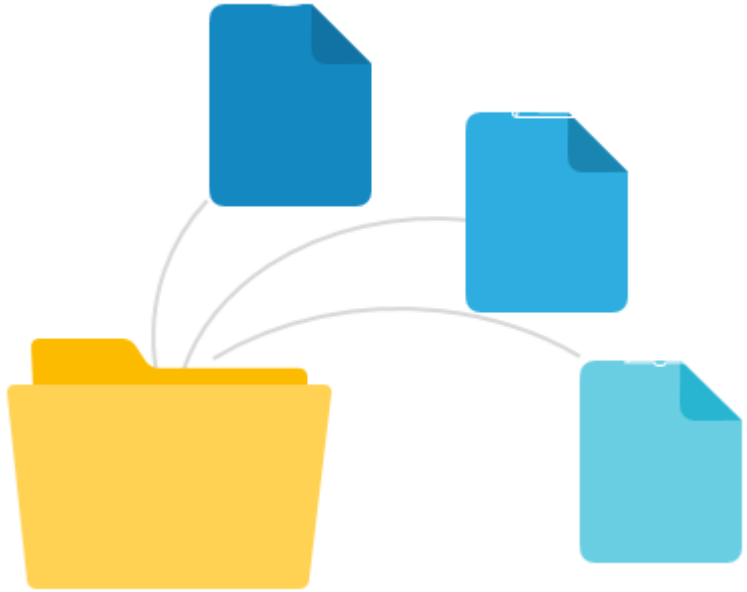
02

- PHẠM VI QUẢN LÝ RỦI RO (QLRR)

03

- CÁC THUẬT NGỮ VÀ ĐỊNH NGHĨA (QLRR)

01



Giới thiệu về Quản lý rủi ro

1.Rủi ro và tầm quan trọng của quản lý rủi ro đối với doanh nghiệp

2.Tầm quan trọng của Quản lý rủi ro và An toàn thông tin trong doanh nghiệp

3.Tính hai mặt và thuộc tính của rủi ro

1. Rủi ro và tầm quan trọng của QLRR đối với doanh nghiệp(1)

1.1 Rủi ro là gì?

- **Rủi ro là tác động (hay ảnh hưởng, hiệu ứng, tác dụng…) của sự không chắc chắn lên mục tiêu (Risk is effect of uncertainty on objectives (ISO 31000:2018))** (*)

Chú thích 1: Ảnh hưởng (hay tác động) của sự không chắc chắn gây ra sự sai lệch so với mục tiêu dự kiến. Ảnh hưởng có thể tích cực, tiêu cực hoặc cả hai và có thể được giải quyết, có thể tạo ra hay dẫn đến cơ hội và mối đe dọa. Sự không chắc chắn là trạng thái, thậm chí là một phần, của sự thiếu hụt thông tin liên quan đến, sự hiểu biết hoặc kiến thức về một sự kiện, hậu quả của nó hoặc khả năng xảy ra

Chú thích 2: Các mục tiêu có thể có những khía cạnh và các phạm trù khác nhau và có thể được áp dụng ở các cấp khác nhau.

1. Rủi ro và tầm quan trọng của QLRR đối với doanh nghiệp(2)

1.1 Rủi ro là gì?

- Trong bối cảnh của các hệ thống quản lý ATTT, rủi ro ATTT có thể được thể hiện dưới dạng tác động của sự không chắc chắn lên các mục tiêu ATTT.
- Rủi ro ATTT liên quan đến khả năng các mối đe dọa khai thác được điểm yếu (hay lỗ hổng bảo mật) của tài sản thông tin xảy ra và hệ quả là tổ chức bị tổn hại (vật chất, danh tiếng, uy tín…).
- Rủi ro kết hợp ba yếu tố: bắt đầu bằng một **sự kiện tiềm ẩn** (“**potential event** ”) và sau đó kết hợp **xác suất xảy ra** (“**probability** or **“likelihood”**) với **mức độ nghiêm trọng** tiềm ẩn (“**potential severity**”) (hay hậu quả “**consequence**” hoặc tác động **“Impact”**).

1. Rủi ro và tầm quan trọng của QLRR đối với doanh nghiệp[3]

1.1 Rủi ro là gì? *(tiếp)*

- Rủi ro kết hợp ba yếu tố: **sự kiện tiềm ẩn** (“**potential event** ” /ɪˈvent/) + **xác suất xảy ra** (“**probability** ” /ˌprɒbəˈbɪləti/) + **mức độ nghiêm trọng** tiềm ẩn (“**potential severity**” /pəˈtenʃəl sɪˈverəti/) (*).

Ví dụ: Sự cố CrowdStrike ngày 19/07/2024

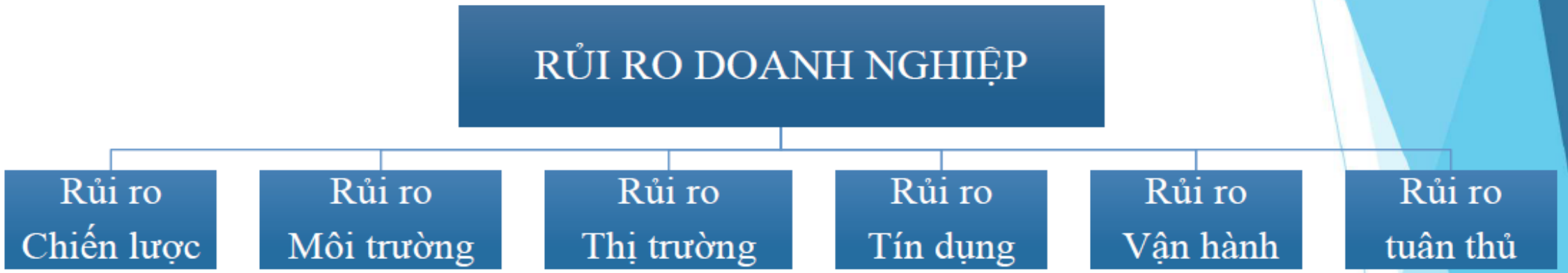
- ***Sự kiện tiềm ẩn*** *(“**potential event** ”): (1) khách hàng thiết lập chế độ cấu hình tự động cập nhật phiên bản mới trên hệ thống; (2) CrowdStrike không có quy trình “System Acceptance Testing”, “Rollback” đạt chất lượng/đáng tin cậy; (3) khách hàng không có hệ thống dự phòng để có thể “failover”; (4) …*
- ***Xác suất xảy ra*** *(“**probability** ”): Bản cập nhật phần mềm Falcon (của CrowdStrike) có lỗi;*
- ***Mức độ nghiêm trọng*** *(“**severity**”) : khoảng 8,5 triệu máy tính chạy Windows OS ở nhiều nước trên thế giới sau khi cập nhật phần mềm đã đột ngột gặp sự cố “blue screen of death” vào sáng 19/07/2024 (~ máy tính ngừng hoạt động).*

1. Rủi ro và tầm quan trọng của QLRR đối với doanh nghiệp[4]

1.2 Tầm quan trọng của QLRR đối với doanh nghiệp

- Tạo ra một môi trường làm việc an toàn và bảo mật cho tất cả nhân viên và khách hàng;
- Tăng tính ổn định của hoạt động kinh doanh;
- Bảo vệ doanh nghiệp khỏi những sự kiện có hại, rủi ro từ môi trường;
- Bảo vệ tất cả những người có liên quan và tài sản khỏi bị tổn hại;
- Tiết kiệm phí bảo hiểm không cần thiết.

2.Tầm quan trọng của QLRR ATTT trong doanh nghiệp[1]



Rủi ro liên quan đến CNTT

Hoạt động cung cấp dịch vụ CNTT (Rủi ro từ các dịch vụ không đáp ứng SLA, không đáp ứng ATTT…)

Triển khai các dự án CNTT (Các dự án khi triển khai gặp rủi ro về tiến độ, phạm vi, chất lượng, chi phí …)

An toàn Thông tin (Rủi ro phát sinh làm tổn hại đến 3 trụ cột (pillars) của ATTT (A-I-C) trong doanh nghiệp)

2.Tầm quan trọng của QLRR ATTT trong doanh nghiệp(2)

- Phát hiện sớm hơn sự tổn hại các tài sản của doanh nghiệp;
- Giảm thiểu hoặc hạn chế tối đa tổn thất;
- Chủ động phản ứng với các mối đe dọa tiềm tàng;
- Nhận diện và ưu tiên nguồn lực ứng phó với rủi ro ảnh hưởng đến mục tiêu;
- Tuân thủ pháp luật và quy định của cơ quan quản lý cấp trên;
- Tăng khả năng thành công của các dự án CNTT;

2.Tầm quan trọng của QLRR ATTT trong doanh nghiệp[3]

- Cải thiện hiệu suất làm việc, nâng cao niềm tin của các bên liên quan;
- Xây dựng văn hóa và nâng cao nhận thức rủi ro;
- Giảm sự lệ thuộc vào chuyên gia;
- Kiểm soát sự cố giúp hoạt động kinh doanh liên tục tốt hơn;
- Tiếp cận QLRR giúp cải thiện chất lượng ra quyết định của cấp quản trị (Board of Directors - BoD/ Board of Management - BoM);
- Nâng cao hiệu quả đáp ứng tích cực của cấp quản trị với đề xuất của cấp dưới;
- …

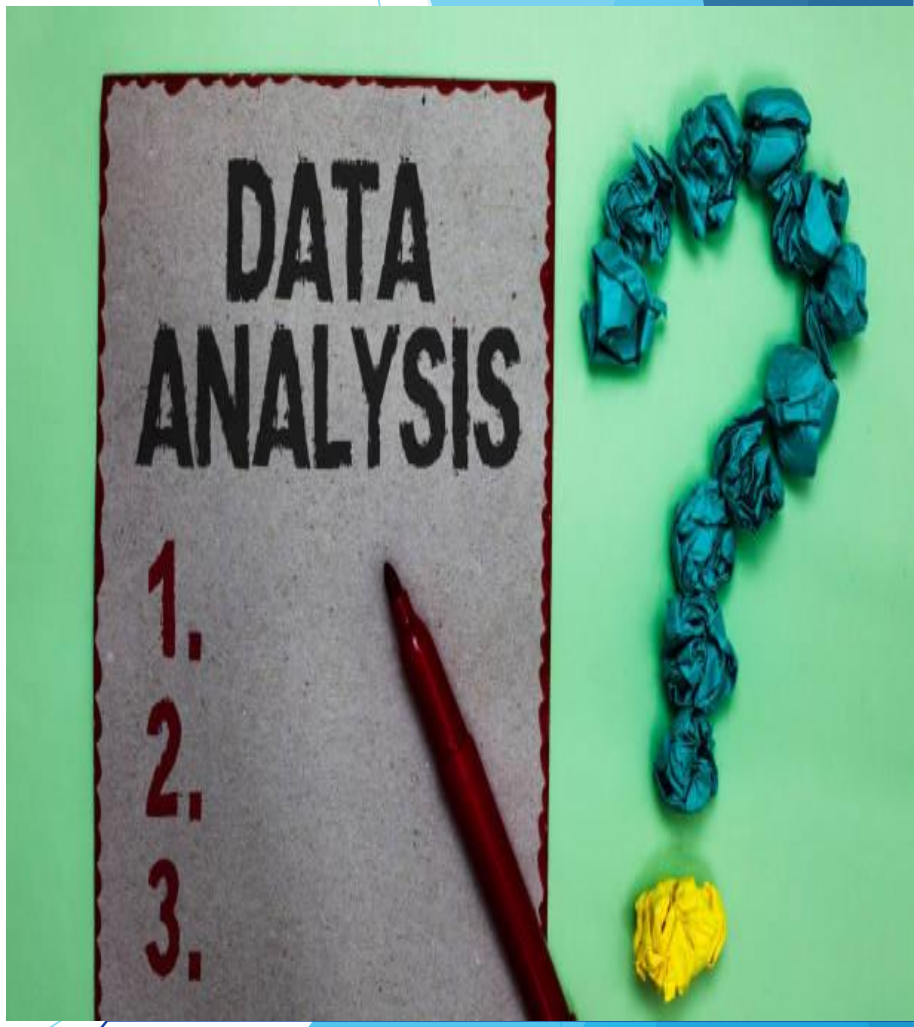
3.Tính hai mặt và thuộc tính của rủi ro(1)

- Tính hai mặt của rủi ro
  - Rủi ro có tính hai mặt: mặt tốt lẫn mặt xấu; tích cực lẫn tiêu cực
  - Bộ Tiêu chuẩn ISO 27001:2013 và các tài liệu ISO có liên quan về ATTT xét rủi ro ATTT hoàn toàn theo khía cạnh tiêu cực

3.Tính hai mặt và thuộc tính của rủi ro(2)

- Thuộc tính của rủi ro

  Rủi ro có thể mô tả dưới dạng định tính hoặc định lượng.



02

Phạm vi Quản lý rủi ro (QLRR)

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT)(1)

- Tài liệu học tập này cung cấp các hướng dẫn về **quản lý các rủi ro an toàn thông tin trong doanh nghiệp theo tiêu chuẩn ISO 31000:2018 có kết hợp với ISO 27000:2018, ISO 27001:2013, ISO 27002:2013, ISO 27005:2008 và ISO 22301:2019**. Việc áp dụng các hướng dẫn này có thể được điều chỉnh cho phù hợp với mọi tổ chức trong bối cảnh của nó.
- Sử dụng tiêu chuẩn ISO 31000:2018 về QLRR cung cấp một phương pháp tiếp cận chung để quản lý mọi loại hình rủi ro và không quy định cụ thể cho ngành hoặc lĩnh vực nào.

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT) (2)

- ISO là dạng viết ngắn gọn tên Tổ chức tiêu chuẩn hoá quốc tế (*International Organization for Standardization* –ISO) là cơ quan thiết lập tiêu chuẩn quốc tế bao gồm các đại diện từ các tổ chức tiêu chuẩn các quốc gia. Tổ chức này đã đưa ra các tiêu chuẩn thương mại và công nghiệp trên phạm vi toàn thế giới.
- Việt Nam (đại diện là Tổng cục Tiêu chuẩn Đo lường Chất lượng) đã tham gia ISO từ năm 1977 và hiện là thành viên chính thức.

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT)[3]

Các định nghĩa về an toàn thông tin theo ISO 27000:2018

- An toàn thông tin (viết tắt là ATTT) (còn gọi là bảo mật thông tin) là bảo toàn tính bí mật (3.10), tính toàn vẹn (3.36) và tính sẵn có (3.7) của thông tin (***Information security is preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information***).

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT) (4)

- Tính sẵn có là đặc tính có thể truy cập và sử dụng được theo yêu cầu của một thực thể được ủy quyền (***Availability*** /əˌveɪləˈbɪləti/ *is property of being accessible and usable on demand by an authorized entity)*.

  - Chỉ những ai được cấp quyền hạn phù hợp mới có thể truy cập và sử dụng được thông tin.

  - Thuật ngữ liên quan: *"redundancy, failover, RAID, data recovery and business continuity plan, etc."*

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT) (5)

- Tính toàn vẹn là đặc tính của tính chính xác và đầy đủ (***Integrity*** /ɪnˈtegrəti/ *is property of accuracy and completeness)*.
  - Trong ATTT, tính toàn vẹn có nghĩa rằng thông tin không thể bị chỉnh sửa mà không bị phát hiện. Tính toàn vẹn bị xâm phạm khi một thông điệp bị chỉnh sửa khi truyền nhận thông tin giữa các bên trong giao dịch.
  - Thuật ngữ liên quan: *"version control, access control, security control, data logs, checksums, backup and recovery, etc."*

Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT) (6)

- Tính bảo mật là đặc tính mà thông tin không được cung cấp hoặc tiết lộ cho các cá nhân, tổ chức hoặc quy trình trái phép (3.54) (***Confidentiality*** / /ˌkɒnfɪdenʃiˈæləti/ / *is property that information is not made available or disclosed to unauthorized individuals, entities, or processes (3.54)).*

  - Trong ATTT, tính bảo mật thể hiện bằng biện pháp kiểm soát truy cập thông tin, mã hóa thông tin…

  - Thuật ngữ liên quan: “Encryption, Authentication (2FA), access control lists, file permissions, etc.”

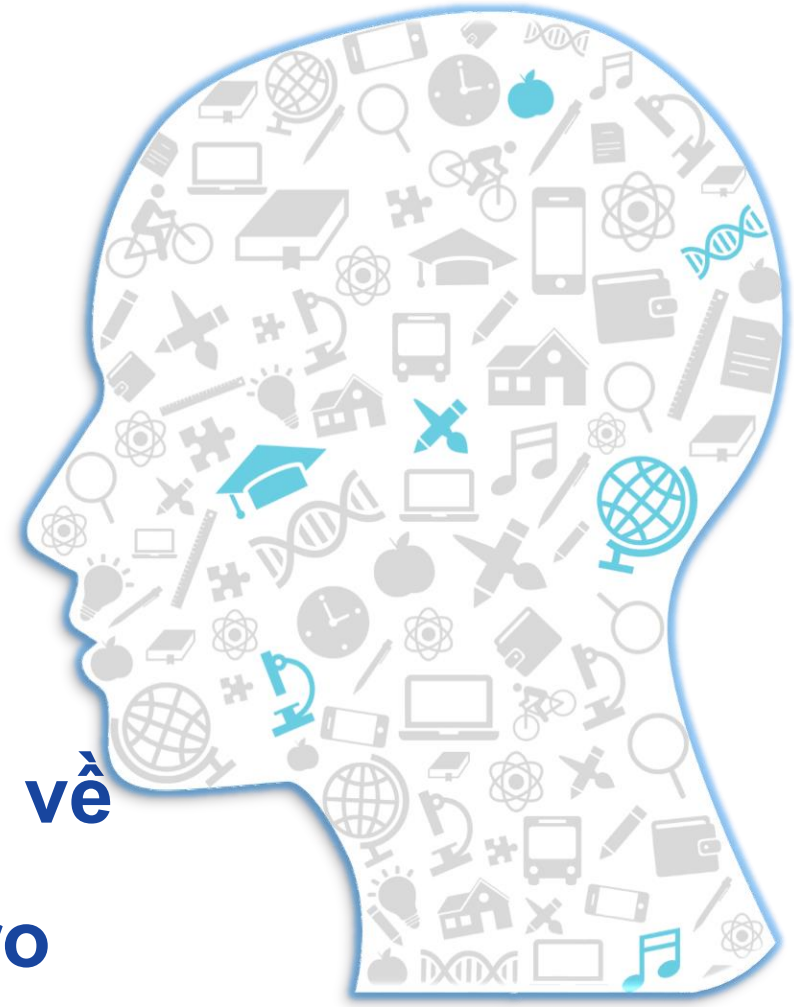
Phạm vi quản lý rủi ro an toàn thông tin (QLRR ATTT) (7)

Bộ ba tính sẵn sàng, tính toàn vẹn và tính bảo mật (A-I-C).

Ba đặc tính này có tài liệu gọi là 3 trụ cột hoặc 3 thành phần hoặc 3 khái niệm hoặc 3 nguyên tắc (pillars/ components/concepts/ principles) của an toàn thông tin (ATTT).

03

Các thuật ngữ và định nghĩa về Rủi ro (RR) và Quản Lý Rủi ro



Các thuật ngữ và định nghĩa

3.1 Risk

- Risk is effect of uncertainty on objectives (*Rủi ro là tác động/ảnh hưởng của sự không chắc chắn lên mục tiêu)* [ISO 31000:2018]

Chú thích 1: Tác động/ảnh hưởng của sự không chắc chắn gây ra sự sai lệch so với mục tiêu dự kiến. Nó có thể tích cực, tiêu cực hoặc cả hai và có thể giải quyết, tạo ra hoặc dẫn đến các cơ hội và mối đe dọa.

Chú thích 2: Sự không chắc chắn là trạng thái, thậm chí là một phần, của sự thiếu hụt thông tin liên quan đến, sự hiểu biết hoặc kiến thức về một sự kiện, hậu quả của nó hoặc khả năng xảy ra.

Chú thích 3: Rủi ro thường được thể hiện dưới dạng **nguồn rủi ro** (3.4), các **sự kiện tiềm ẩn** (3.5), **hậu quả** của chúng (3.6) và **khả năng xảy ra** (3.7) của chúng.

(*)*Sự cố ("incident") là những rủi ro ("risks") đã hiện hữu (thực sự đã xảy ra).*

Các thuật ngữ và định nghĩa(2)

- Risk is effect of uncertainty on objectives (*Rủi ro là tác động/ảnh hưởng của sự không chắc chắn lên mục tiêu)* [ISO 31000:2018]
  - Rủi ro thường được thể hiện dưới dạng sự kết hợp giữa *"hậu quả"* của một sự kiện (bao gồm cả những thay đổi về hoàn cảnh) liên kết với *"khả năng xảy ra"*.
  - Trong bối cảnh của các hệ thống quản lý ATTT, rủi ro ATTT có thể được thể hiện như tác động của sự không chắc chắn đối với các mục tiêu ATTT.
  - **Rủi ro ATTT liên quan đến khả năng tiềm ẩn** ("possibility, likelihood, probability") **của các mối đe dọa sẽ khai thác các điểm yếu (lỗ hổng) của một hoặc một nhóm tài sản thông tin và do đó gây tác động** ("impact, consequence, effect") **cho một tổ chức. >>>** *diễn giải này sẽ được dùng cho các chương sau (*)*

Các thuật ngữ và định nghĩa(3)

3.2 Risk management

Quản lý rủi ro (Risk management) là phối hợp các hoạt động để chỉ đạo và kiểm soát một tổ chức về rủi ro. [ISO 31000:2018]

3.3 Stakeholder /ˈsteɪkˌhəʊl.dər/

Bên liên quan (Stakeholder) là người hoặc tổ chức có thể ảnh hưởng, bị ảnh hưởng, hoặc tự nhận thức là bị ảnh hưởng bởi một quyết định hay hoạt động. [ISO 31000:2018]

3.4 Risk Source

Nguồn rủi ro (Risk source) là yếu tố mà tự thân nó hoặc trong sự kết hợp có thể làm phát sinh rủi ro. [ISO 31000:2018]

Các thuật ngữ và định nghĩa(4)

3.5 Event /ɪˈvent/

Sự kiện (Event) Sự xảy ra (sự xuất hiện) hoặc thay đổi của một tập hợp các tình huống cụ thể. [*occurrence or change of a particular set of circumstances* - ISO 31000:2018] (*)

Chú thích 1: Một sự kiện có thể xảy ra một hoặc nhiều lần và có thể có nhiều nguyên nhân và hệ quả (3.6).

Chú thích 2: Một sự kiện cũng có thể là điều được mong đợi mà không xảy ra, hoặc điều không mong đợi nhưng lại xảy ra.

Chú thích 3: Một sự kiện có thể là một nguồn rủi ro.

[ISO 27000]: “An event can sometimes be referred to as an “incident” or “accident”.”

Các thuật ngữ và định nghĩa(5)

3.6 Consequence /ˈkɒn.sɪ.kwəns/

Hệ quả (Consequence) là kết quả của một sự kiện (3.5) ảnh hưởng đến mục tiêu [*outcome of an event affecting objectives* - ISO 31000:2018]

3.7 Likelihood /ˈlaɪ.kli.hʊd/

Khả năng xảy ra (Likelihood) là cơ hội một điều gì đó xảy ra [*chance of something happening* - ISO 31000:2018]

3.8 Control /kənˈtrəʊl/

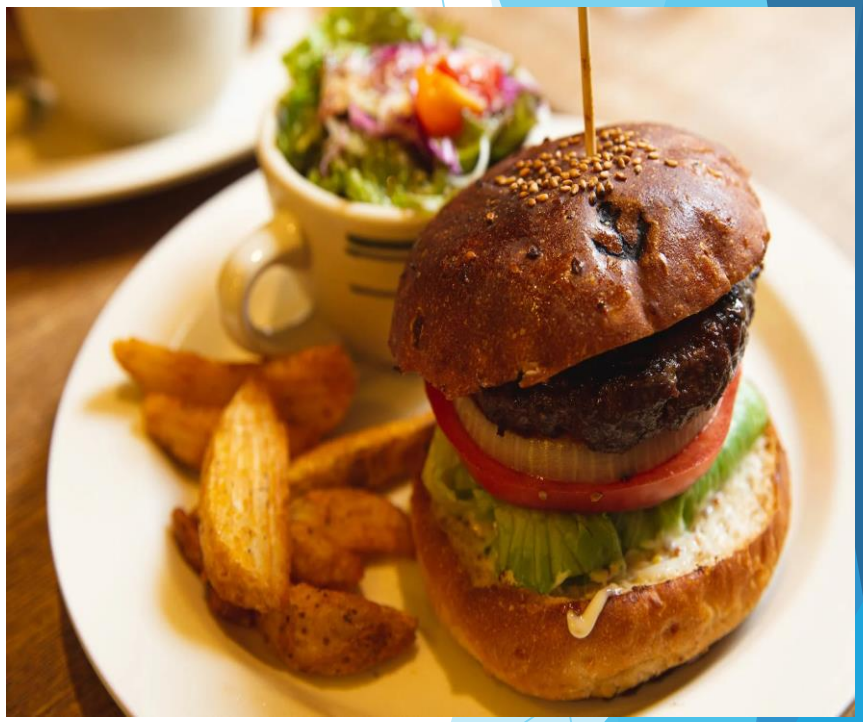
Kiểm soát (Control) là biện pháp duy trì và/hoặc thay đổi các rủi ro (3.1) [*measure that maintains and/or modifies risk* - ISO 31000:2018]

Các thuật ngữ và định nghĩa(6)

3.9 Risk Appetite /ˈæp.ə.taɪt/

Khẩu vị rủi ro (Risk Appetite)

- Khẩu vị rủi ro là lượng và loại rủi ro mà một tổ chức sẵn sàng chấp nhận để đạt được các mục tiêu chiến lược của mình.



Các thuật ngữ và định nghĩa(7)

3.10 Risk Tolerance

Khả năng chịu đựng rủi ro (Risk Tolerance)

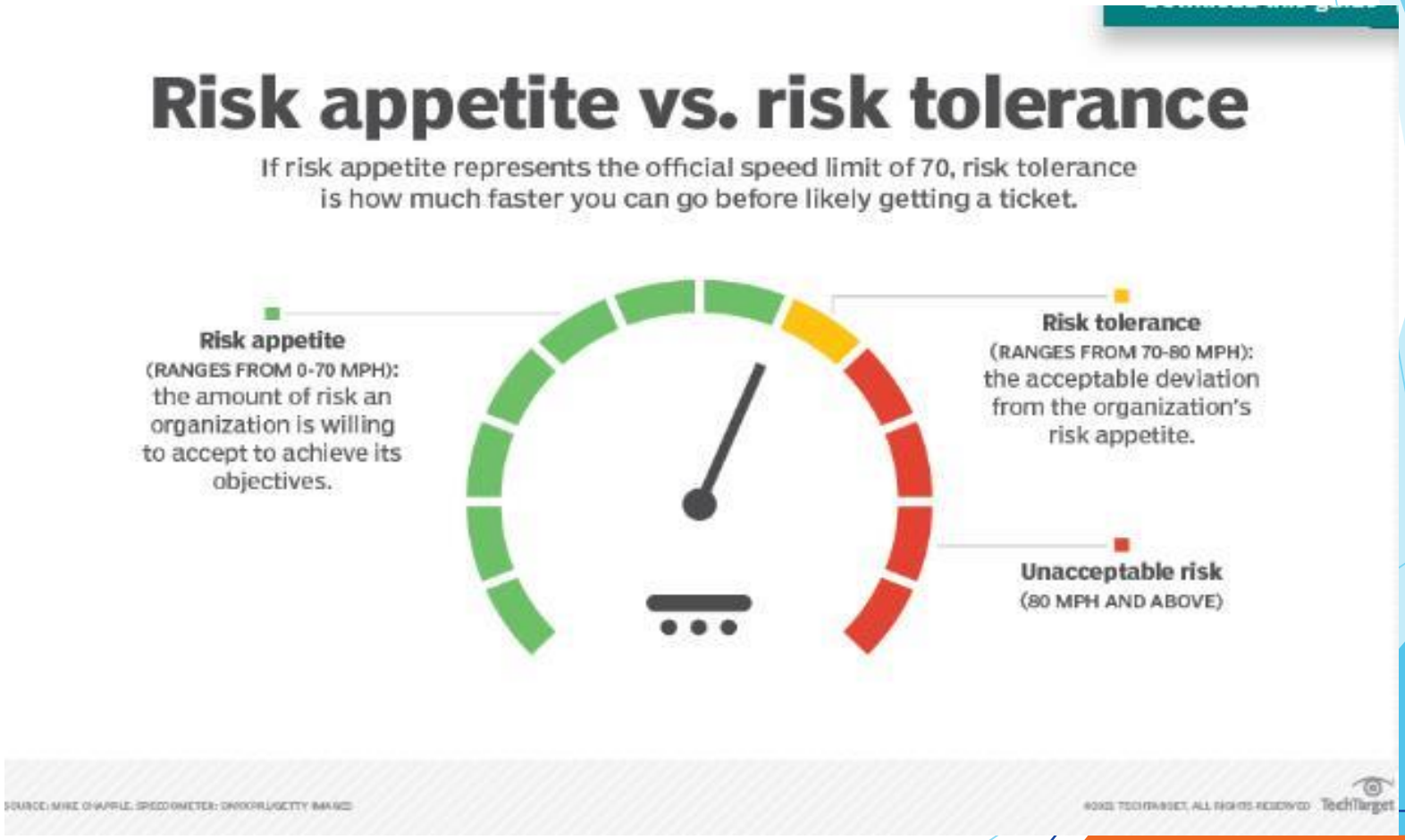
Mức độ rủi ro mà một thực thể sẵn sàng chấp nhận để đạt được kết quả mong muốn tiềm năng.

(*)Có tài liệu gọi "Risk Tolerance" là "Biên độ rủi ro" hay "Độ giãn rủi ro cho phép".

- *Biên độ rủi ro là mức sai lệch thực tế cho phép so với khẩu vị rủi ro tiêu chuẩn đã được phê duyệt nhằm xem xét việc chấp nhận một rủi ro cụ thể.*
- *Tổng của Khẩu vị rủi ro và Biên độ rủi ro không được phép vượt quá Giới hạn rủi ro.*

Các thuật ngữ và định nghĩa[8]

- Risk Appetite vs. Risk Tolerance



Các thuật ngữ và định nghĩa[9]

3.11 Risk Attitude

Thái độ rủi ro (Risk Attitude /ˈæt.ɪ.tʃuːd/):

-Thái độ rủi ro là "phản ứng được lựa chọn (của ai đó) đối với sự không chắc chắn có ý nghĩa (đối với họ); phản ứng này chịu ảnh hưởng của nhận thức (của họ) *("Risk attitude is "chosen response to uncertainty that matters, influenced by perception"").* *[https://pmstudycircle.com/risk-attitude/]*

-Thái độ rủi ro đề cập đến sự sẵn lòng và sở thích của các bên liên quan đối với rủi ro. Nó phản ánh cách một người nhận thức và tiếp cận rủi ro và kết quả tiềm năng trong quá trình ra quyết định.

Các thuật ngữ và định nghĩa(10)

➢ Thái độ rủi ro (Risk Attitude):

Thái độ rủi ro là khuynh hướng (Tránh rủi ro, Tìm kiếm hoặc chấp nhận rủi ro, Trung lập rủi ro và Chấp nhận rủi ro) đối với sự không chắc chắn (hay rủi ro), được các cá nhân và nhóm chấp nhận một cách rõ ràng hoặc ngầm định, được thúc đẩy bởi nhận thức và được chứng minh bằng hành vi có thể quan sát được.

Các thuật ngữ và định nghĩa(11)

- **Thái độ rủi ro (Risk Attitude):**

- Risk-averse /əˈvɜːs/ : không thích (có) rủi ro

(*) Người lao động nên thận trọng và cảnh giác trong lời nói nếu chủ doanh nghiệp của họ là người không thích nghe ai nói về rủi ro tại nơi làm việc. Người nào hay nói về rủi ro sẽ bị chủ doanh nghiệp gán tội là 'hay nói chuyện xui xẻo' / 'gieo rắc nỗi sợ hãi' trong doanh nghiệp.

Các thuật ngữ và định nghĩa[11]

➢ Thái độ rủi ro (Risk Attitude):

- Risk-seeker: chấp nhận rủi ro như là cơ hội thách thức để giải quyết.
- Risk-neutral /ˈnjuː.trəl/ : trung lập với rủi ro, đối phó với rủi ro một cách khách quan.
- Risk-tolerant /ˈtɑː.lə͡ɹ.ənt/ : không chú ý đến rủi ro cho đến khi rủi ro trở thành vấn đề.

Các thuật ngữ và định nghĩa(12)

3.12 Residual Risk

Rủi ro còn lại (Residual Risk - /rɪˈzɪdʒ.ju.əl/ /risk/):

Rủi ro còn lại sau khi xử lý rủi ro (“Risk (3.61) remaining after risk treatment (3.72)”) [ISO 27000:2018]

Note 1 to entry: Residual risk can contain unidentified risk.

Note 2 to entry: Residual risk can also be referred to as “retained risk”.

ví dụ: với mục tiêu duy trì hoạt động liên tục cho máy tính thì việc sử dụng UPS cho máy tính không triệt tiêu rủi ro cố hữu liên quan đến nguồn điện cung cấp và chất lượng UPS.

Các thuật ngữ và định nghĩa(13)

3.13 Risk Criteria

Tiêu chí rủi ro (Risk criteria /risk kraɪˈtɪəriən/) là điều khoản tham chiếu dựa vào đó đánh giá mức độ (cao/thấp), tầm quan trọng (ý nghĩa) của rủi ro (3.61) (terms of reference against which the significance of risk (3.61) is evaluated) [ISO 27000:2018].

Note 1 to entry: Risk criteria are based on organizational objectives, and external context (3.22) and internal context (3.38).

Note 2 to entry: Risk criteria can be derived from standards, laws, policies (3.53) and other requirements (3.56) (or measures, or expectations)

Các thuật ngữ và định nghĩa(14)

3.13 Risk Criteria *(tiếp)*

- Tiêu chí rủi ro là các tiêu chuẩn thể hiện quan điểm của cá nhân (hoặc quan điểm của cơ quan quản lý) về mức độ rủi ro có thể chấp nhận/chịu đựng được.
- Thiết lập tiêu chí rủi ro là phương pháp phổ biến của doanh nghiệp để thể hiện khả năng chấp nhận rủi ro của một cá nhân lãnh đạo hoặc của tổ chức trong quá trình ra quyết định:
  - rủi ro có thể chấp nhận được;
  - rủi ro không thể chấp nhận được; hay
  - rủi ro cần giảm xuống mức thấp nhất có thể thực hiện được một cách hợp lý.

Các thuật ngữ và định nghĩa(15)

3.13 Risk Criteria *(tiếp)*

- Mức độ rủi ro có thể chấp nhận/chịu đựng được dựa vào việc đánh giá mức độ (cao/thấp) của các yếu tố sau:
  - Khả năng xảy ra ('Likelihood / Probability') rủi ro;
  - Hậu quả/Tác động ('Consequence / Impact') của rủi ro;
  - Hiệu quả kiểm soát ('Control effectiveness') rủi ro;
  - Xếp hạng rủi ro ('Risk rating')

Ví dụ: Tiêu chí rủi ro thường được xếp hạng theo thứ tự Thấp (Low) → Trung bình (Medium) → Cao (high) theo xếp hạng của Khả năng xảy ra (Likelihood) và Hệ quả (hay tác động) (Consequence/Impact). Sau đây là ví dụ minh họa cho tiêu chí rủi ro từ slide 38 – 40:

Các thuật ngữ và định nghĩa(16)

3.13 Risk criteria *(tiếp)* – *Risk matrix*

Xếp hạng rủi ro, khả năng xảy ra và hậu quả được trình bày theo ma trận rủi ro:

Consequences / Impact							
	Catastrophic	5	5	10	15	20	25
	Major	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	Insignificant	1	1	2	3	4	5
			1	2	3	4	5
			Rare	Unlikely	Possible	Likely	Almost certain
Likelihood / Probability							

Các thuật ngữ và định nghĩa(17)

3.13 Risk criteria *(tiếp)*

	Xếp hạng rủi ro	Khả năng chấp nhận rủi ro	Hành động được khuyến nghị	
Màu đỏ	Rất cao	Không thể chấp nhận	Phải có biện pháp giảm rủi ro *(risk reducing measures must be implemented)*	MUST/ SHALL
Màu cam	Cao	Không thể chấp nhận	Nên có biện pháp giảm rủi ro *(risk reducing measures should be implemented)*	SHOULD
Màu vàng	Trung bình	Trung bình	Biện pháp giảm rủi ro có thể có *(risk reducing measures can be implemented)*	CAN
Màu xanh	Thấp	Có thể chấp nhận	Không cần có biện pháp giảm rủi ro *(risk reducing measures are not required)*	To be

Các thuật ngữ và định nghĩa(18)

3.13 Risk criteria *(tiếp)*

Tác động/ Hậu quả	Xếp hạng rủi ro	Khả năng chấp nhận rủi ro	Hành động được khuyến nghị	
Tổn thất 10 tỷ – 50 tỷ VNĐ	Rất cao	Không thể chấp nhận	Phải có biện pháp giảm rủi ro *(risk reducing measures must be implemented)*	MUST/ SHALL
Tổn thất 5 tỷ – 10 tỷ VNĐ	Cao	Không thể chấp nhận	Nên có biện pháp giảm rủi ro *(risk reducing measures should be implemented)*	SHOULD
Tổn thất 1 tỷ – 5 tỷ VNĐ	Trung bình	Trung bình	Biện pháp giảm rủi ro có thể có *(risk reducing measures can be implemented)*	CAN
Tổn thất 500 triệu – 1 tỷ đồng	Thấp	Có thể chấp nhận	Không cần có biện pháp giảm rủi ro *(risk reducing measures are not required)*	To be

Các thuật ngữ và định nghĩa(19)

3.14 Risk Assessment - Risk Evaluation

+ Risk Assessment is overall process (3.54) of risk identification (3.68), risk analysis (3.63) and risk evaluation (3.67)

+ Risk Evaluation is process (3.54) of comparing the results of risk analysis (3.63) **with risk criteria** (3.66) to determine whether the risk (3.61) and/or its magnitude is acceptable or tolerable.

Note 1 to entry: Risk evaluation assists in the decision about risk treatment (3.72)

Các thuật ngữ và định nghĩa(20)

3.15 Performance

Kết quả có thể đo lường được (Performance /pəˈfɔː.məns/)

- measurable result [ISO 27000:2018]

Note 1 to entry: Performance can relate either to quantitative or qualitative findings.

Note 2 to entry: Performance can relate to the management of activities, processes (3.54), products (including services), systems or organizations (3.50).

Các thuật ngữ và định nghĩa(21)

3.16 Policy

Chính sách (policy /ˈpɒl.ə.si/)

- Intentions and direction of an organization, as formally expressed by its top management *(Ý định và chỉ đạo của một tổ chức, được thể hiện chính thức bởi ban quản lý cấp cao của tổ chức đó)*

[ISO 27000:2018]

- A statement of objectives, rules, practices or regulations governing the activities of people within a certain context.*(Một tuyên bố về các mục tiêu, quy tắc, thông lệ hoặc quy định chi phối các hoạt động của mọi người trong một bối cảnh nhất định.)*

[Read more at Policy - Glossary | CSRC (nist.gov)]

Các thuật ngữ và định nghĩa(22)

3.17 Process

Quá trình / quy trình (process /ˈprəʊ.ses/)

A sequence of activities that use inputs to deliver an intended result *(Một chuỗi các hoạt động sử dụng đầu vào để mang lại kết quả mong muốn)* [ISO 9001:2015]

Ví dụ: quá trình / quy trình mua sắm thiết bị; quy trình đấu thầu dự án; …

Các thuật ngữ và định nghĩa(23)

3.18 Procedure

Thủ tục (Procedure /prəˈsiː.dʒər/)

- a defined way to execute an activity or a process. Procedures can be documented or not.[ISO 9001:2015]
- a usually fixed or ordered series of actions or events leading to a result *[https://www.merriam-webster.com/thesaurus/procedure]*
- a set of actions that is the official or accepted way of doing something *[https://dictionary.cambridge.org/dictionary/english/procedure]*

Các động từ cần chú ý khi đọc tài liệu ISO (24)

3.19 “shall” indicates a requirement;

E.g. The organization shall implement and maintain a process to manage risks

3.20 “should” indicates a recommendation;

E.g. The principles are the foundation for managing risk and should be considered when establishing the organization’s risk management processes.

3.21 “may” indicates a permission;

3.22 “can” indicates a possibility or a capability.

Tài liệu tham khảo QLRR ATTT

1. ISO 31000:2018 Risk management — Guidelines

2. ISO 27000:2018 Information technology — Security techniques — Information security management systems — **Overview and vocabulary**

3. ISO/IEC 27001:2013 Information technology — Security techniques - Information security management systems – Requirements

4. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

5. BS ISO/IEC 27005:2008 Information technology — Security techniques —Information security risk management

6. ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

v.v.

Hết Chương 01

Cám ơn tất cả Anh/Chị đã theo dõi Chương này

(*)Một số hình minh họa được tải từ trang https://www.pexels.com/ và https://pixabay.com/