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 9
CHỈ SỐ RỦI RO TRỌNG YẾU
(Key Risk Indicator)

Nội dung

01 Khái quát về KPI và KRI (General)

02 Phân biệt KPI và KRI

03 Cách thiết lập và phát triển KRI

04 Các chỉ số rủi ro trọng yếu (KRI) tiêu biểu

01

Khái quát (General)

Chỉ số hiệu suất công việc trọng yếu (KPI)[1]

- KPI là chữ cái viết tắt của cụm từ Key Performance Indicator. KPI được hiểu là chỉ số đánh giá hiệu quả công việc trọng yếu;
- KPI là công cụ đo lường, đánh giá hiệu quả và hiệu suất ('effectiveness and efficiency') hoàn thành công việc.
- KPI trả lời cho câu hỏi *'how well something is being done'*.

Chỉ số hiệu suất công việc trọng yếu (KPI) (2)

- KPI thường được thể hiện qua số liệu, tỉ lệ (%), chỉ tiêu định lượng, nhằm phản ảnh hiệu quả hoạt động của các cá nhân, các nhóm hoặc bộ phận lao động của doanh nghiệp.

www.flickr.com

Chỉ số hiệu suất công việc trọng yếu (KPI) (3)

➢ **Vai trò KPI:**

Các chỉ số KPI giúp doanh nghiệp theo dõi, đánh giá được hiệu quả của chiến lược kinh doanh, kết quả thực hiện công việc của người lao động một cách minh bạch, rõ ràng, cụ thể, công bằng nhờ các số liệu cụ thể; nhờ đó doanh nghiệp có thể:

- Hoạch định lại chiến lược kinh doanh;
- Đánh giá chính xác năng lực người lao động để có thể khen thưởng hoặc huấn luyện lạo cho người lao động.

Chỉ số hiệu suất công việc trọng yếu (KPI) (4)

➢ Ví dụ một mẫu KPI tại một doanh nghiệp

Logo của đơn vị

BẢNG THIẾT LẬP VÀ ĐÁNH GIÁ KPI CBNV

Kỳ đánh giá: 2020

Họ tên CBNV: TRẦN VĂN CƯỜNG — Khối/Chi nhánh/Phòng giao dịch: Khối CNTT

Chức danh: Nhân viên phụ trách hệ thống mạng (LAN/WAN) — Trung tâm/Phòng/Ban/Bộ phận: Phòng quản lý và vận hành Mạng

Lưu ý:

- Chỉ được cập nhật và chỉnh sửa thông tin của các dòng thuộc nhóm ***A. Mục tiêu công việc*** có STT từ 1 đến 8.
- Đăng ký tối thiểu 3 Mục tiêu và tối đa 8 Mục tiêu cho nhóm ***A. Mục tiêu công việc***
- Yêu cầu cập nhật đầy đủ thông tin ***Cột (1)*** → ***Cột (11)*** tại Thẻ tập KPI
- Bổ sung thông tin ***Cột (12)*** → ***Cột (14)*** tại Thẻ tập KPI chỉ nhập thông tin các Cột (11), (12) và (13) khi thực hiện đánh giá KPI cuối năm.
- Các ô Excel bị khóa là các nội dung không cho phép cập nhật thông tin.
- Tổng trọng số nhóm ***A. Mục tiêu công việc*** là 100%

I. Mục tiêu công việc:

Stt	Mục tiêu công việc	Đơn vị tính	Trọng số	Chỉ tiêu		Thang điểm đánh giá					Điểm đánh giá cuối năm		
				Kết quả năm trước	Chỉ tiêu kế hoạch	Không đạt yêu cầu (1 điểm)	Cần cải tiến (2 điểm)	Đạt yêu cầu (3 điểm)	Giỏi (4 điểm)	Xuất sắc (5 điểm)	Kết quả thực hiện	Điểm cá nhân tự đánh giá	Điểm cấp Quản lý đánh giá
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)
A	**Mục tiêu công việc:**		#####										
1	Tỷ lệ thực hiện thành công kế hoạch hành động theo deadline	Tiến độ thực hiện	10%		100% thiết bị cơ điện được bảo trì; ngân sách sửa chữa nhỏ giảm 20% so với năm trước và KHÔNG PHÁT SINH hạng mục mới	Thực hiện < 80%	80% <= Thực hiện < 90%	90% <= Thực hiện < 100%	Thực hiện = 100%	Thực hiện = 100% và có 10% CV hoàn thành trước hạn			
2	Triển khai thành công các dự án theo Phụ lục đính kèm	ngày	10%		Hoàn thành kế hoạch theo lộ trình trong năm 2019	Thực hiện < 80%	80% <= Thực hiện < 90%	90% <= Thực hiện < 100%	Thực hiện = 100%	Thực hiện = 100% và có 10% CV hoàn thành trước hạn			
3	Xây dựng quy trình (áp dụng đối với Quy trình viết mới và sửa đổi) mới		10%		Theo danh sách DL Quy trình	Thực hiện < 80%	80% <= Thực hiện < 90%	90% <= Thực hiện < 100%	Thực hiện = 100%	Thực hiện > 100%			

Chỉ số rủi ro trọng yếu (KRI)[1]

Chỉ số rủi ro trọng yếu (KRI) *(từ tiếng Anh "Key Risk Indicator")*:

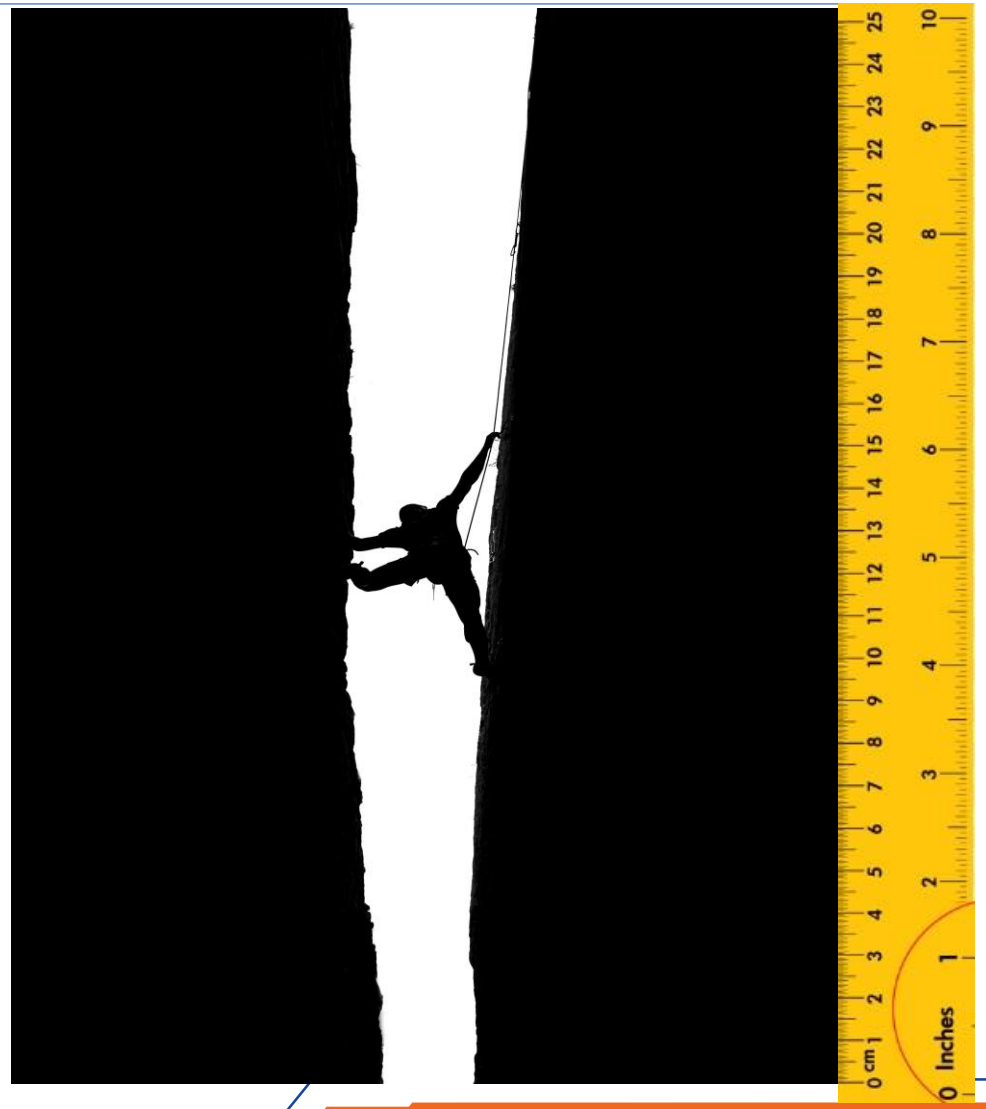
(1) KRI là thước đo *('measure')* được sử dụng trong quản lý để chỉ ra mức độ rủi ro của một hoạt động *('how risky an activity is'?)*.

(2) KRI là tập số liệu *('metrics')* phát ra tín hiệu sớm về mức độ rủi ro ngày càng tăng trong nhiều lĩnh vực hoạt động khác nhau của doanh nghiệp.

Flyingskystone

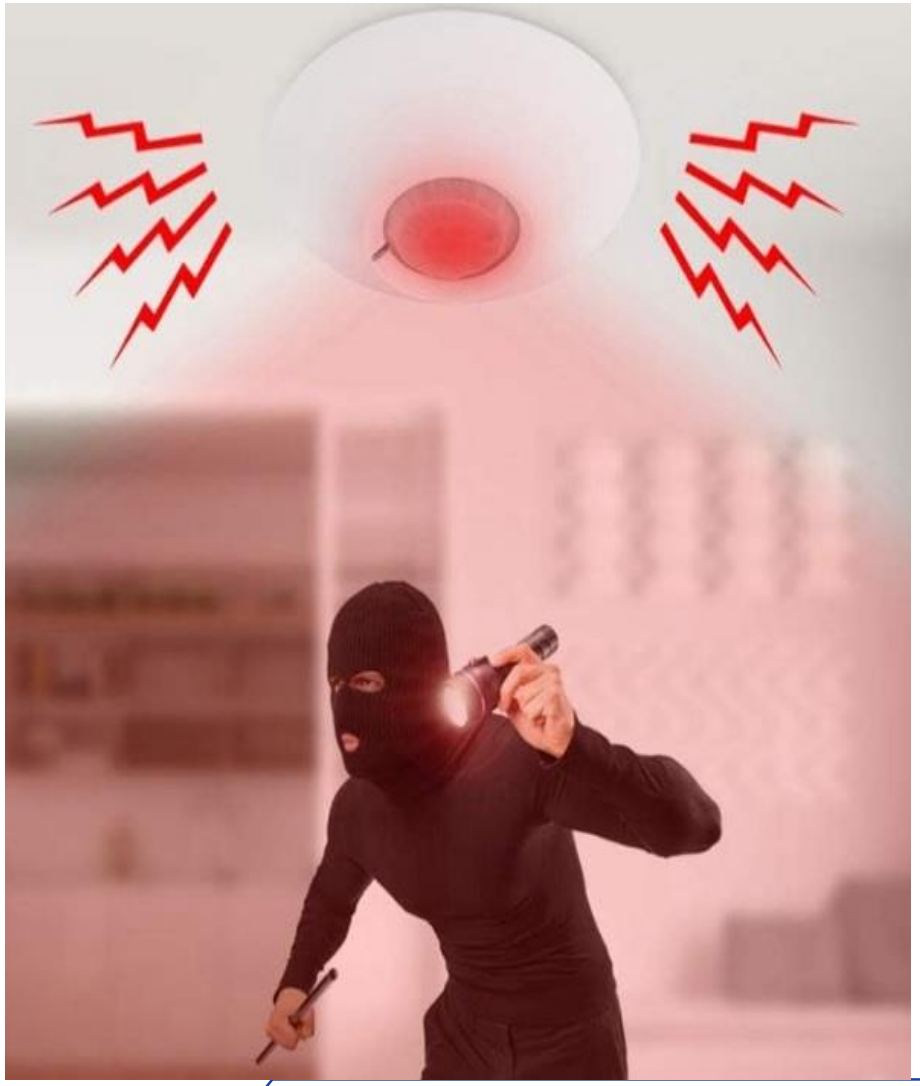
Chỉ số rủi ro trọng yếu (KRI)(2)

(3) KRI là *'metric/metrics'* (số liệu/tập các số liệu) đo lường khả năng xảy ra một sự kiện mà ***xác suất xảy ra*** (Occ) kết hợp với ***hậu quả có mức độ nghiêm trọng*** (Sev) có thể vượt quá mức chấp nhận rủi ro của doanh nghiệp và có tác động tiêu cực sâu sắc đến khả năng thành công của doanh nghiệp.



Chỉ số rủi ro trọng yếu (KRI)[3]

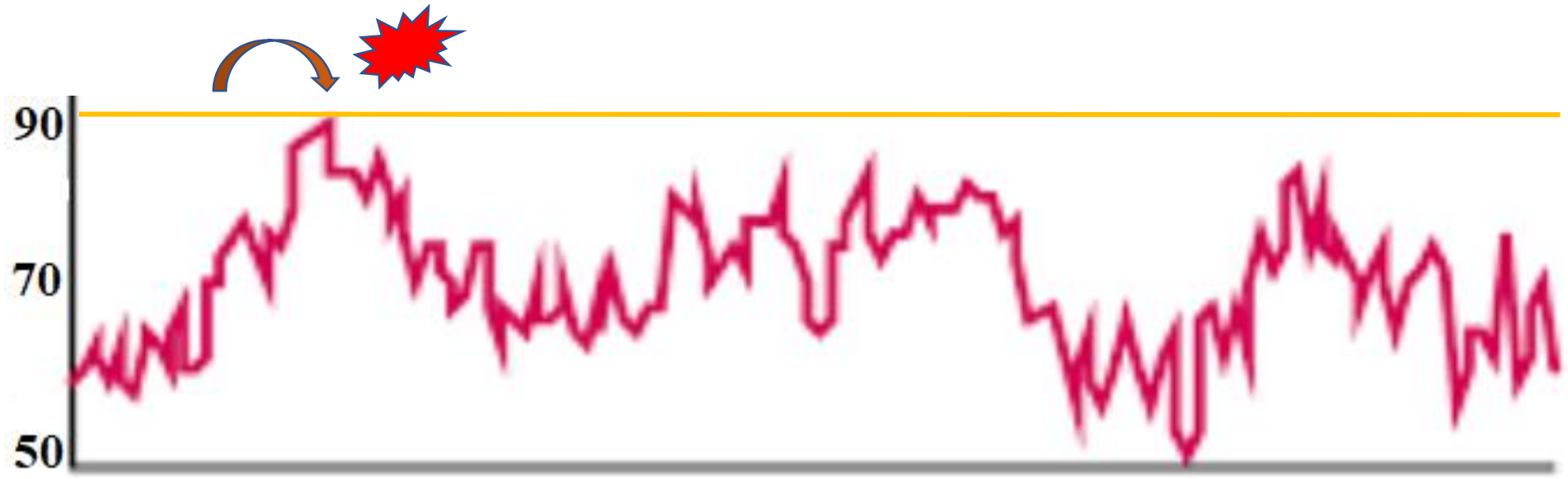
(4) KRI là *'metric/metrics'* được sử dụng để đo lường và giám sát mức độ rủi ro ***('measure and monitor the level of risk')*** liên quan đến một quy trình, hoạt động hoặc hệ thống cụ thể trong một tổ chức. KRI thường được sử dụng trong quản lý rủi ro để cung cấp các dấu hiệu cảnh báo sớm về các rủi ro tiềm ẩn ***('warning signs of potential risk')*** và giúp các tổ chức thực hiện các bước chủ động để giảm thiểu rủi ro.



https://ubuy.vn

Chỉ số rủi ro trọng yếu (KRI)(4)

- KRI được sử dụng để trả lời câu hỏi: *"Rủi ro đang thay đổi như thế nào và nó có nằm trong mức độ chấp nhận mong muốn của chúng ta không?"* (*"How is our risk profile changing, and is it within our desired tolerance levels?"*).



Chỉ số rủi ro trọng yếu (KRI)(5)

- Sử dụng KRI có thể giúp các tổ chức hiểu rõ hơn về rủi ro và quản lý rủi ro. Theo dõi KRI, các tổ chức có thể xác định các vấn đề tiềm ẩn *('potential issues')* trước khi chúng trở thành vấn đề lớn *('major problems')* và thực hiện các bước chủ động để giảm thiểu những rủi ro đó; giúp cải thiện quản lý rủi ro tổng thể, giảm tác động tiềm ẩn của rủi ro đối với tổ chức và ra quyết định chiến lược.

Các thước đo rủi ro(1)

Rủi ro được đo lường bằng Occ, Sev, Det, RPN và KRI:

- Occ đo lường khả năng xảy ra rủi ro "***how likely*** *is it?*";
- Sev đo lường mức độ nghiêm trọng của rủi ro "***How seriously*** *is it?*";
- Det đo lường khả năng phát hiện sớm rủi ro "***How soon*** *can you detect it? /* ***How quickly*** *can you detect it?).*"
- RPN đo lường tác động tổng hợp của rủi ro: RPN = Occ*Sev*Det
- KRI đo lường mức độ rủi ro (cao/thấp) của một hoạt động *('how risky an activity is? / 'how risky is it to do that?')*.

Các thước đo rủi ro(2)

Rủi ro được đo lường bằng Occ, Sev, Det, RPN và KRI:

- Occ, Sev và Det được đo lường bằng cách gán giá trị xếp hạng theo thang điểm từ 1 (Tốt nhất) đến 5 (hoặc 6) (Xấu nhất) – tùy theo thang đo 5 cấp hay 6 cấp (hoặc 10 cấp);
- **RPN** được đo lường theo công thức: **RPN = Occ*Sev*Det**
- **KRI là con số thường được đo lường hoặc tính bằng một công thức tính hoặc được chỉ định bằng một con số cố định**.

Các thước đo rủi ro(3)

Rủi ro được đo lường bằng Occ, Sev, Det, RPN và KRI:

- **KRI** thường được kiểm soát bằng giá trị ngưỡng (hay ngưỡng giá trị). Khi giá trị KRI vượt quá ngưỡng giá trị, rủi ro sẽ xảy ra cho doanh nghiệp.
- Giá trị ngưỡng hay ngưỡng giá trị KRI là một con số hoặc một khoảng (x,y) hay một đoạn [x,y] hay nửa đoạn [x,y) / (x,y] cố định được quy định theo 'Risk Appetite' và 'Risk Tolerance' của lãnh đạo doanh nghiệp.

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (1)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (***"how risky is an activity?"***) (***cao hay thấp?)***

  Ví dụ:

  (1) Dung lượng trống của ổ cứng (HDD) máy tính: **RỦI RO** không đủ dung lượng để sao chép dữ liệu lớn.

  Metrics (tập số liệu %):

  0.1% - 0.2 % - 0.3% - 0.4% - **0.5%** - 0.6% - 0.7% - 0.8% - 0.9% - 1.5%

  KRI = 0.5% x (tổng dung lượng): là giới hạn dung lượng còn lại của HDD, hệ thống sẽ có cảnh báo cho người dùng phải kiểm tra và có biện pháp tăng dung lượng cho HDD hoặc thay HDD mới: giá trị càng tiến đến gần 0.5 thì khả năng xảy ra rủi ro (Occ) tăng lên

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (2)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (***"how risky is an activity?"***) (***cao hay thấp?)***

Ví dụ:

(2) Tốc độ xe ô tô chạy trên đường liên tỉnh: **RỦI RO** bị phạt hay gặp tai nạn trên đường đi.

KRI = 60km/h chính là giới hạn tốc độ (ví dụ 60km/h) mà người lái xe phải chú ý vì nếu vượt qua giới hạn này thì sẽ gặp rủi ro như tai nạn hoặc bị cảnh sát giao thông phạt.

Metrics (tập số liệu tốc độ):

30 Km/h – 40 – 50 – **60** – 65 - 70 – 75 – 80 – 85 – 90 Km/h

:giá trị càng tiến đến gần 60 thì khả năng xảy ra rủi ro (Occ) tăng lên

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (3)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (***"how risky is an activity?"***) (***cao hay thấp?)***

  Ví dụ:

  (3) Số lần đăng nhập (Sign In) vào hệ thống CNTT (hay hệ thống thanh toán của Ngân hàng) thất bại: RỦI RO không vào được hệ thống để làm việc hoặc giao dịch.

  KRI = 5 chính là giới hạn (hay ngưỡng) số lần nhập sai thông tin xác thực (như user name, password):

  lần 1 - lần 2 – lần 3 – lần 4 – **lần 5**

  :giá trị càng đến gần lần 5 thì khả năng xảy ra rủi ro (Occ) tăng lên

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (4)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (***"how risky is an activity?"***) (***cao hay thấp?)***

  Ví dụ:

  (4) Độ bão hòa oxy trong máu ngoại vi ((SpO2) – 'Saturation of peripheral oxygen'): RỦI RO thiếu oxy máu (suy hô hấp) do không thể trao đổi khí Oxy và CO^2 của con người

  Metrics (tập số liệu %):

  90% - 93% - 94% - 95 % - 96% - 97% - 99% - 100%

  KRI = 90% chính là dấu hiệu hay ngưỡng cảnh báo nồng độ oxy trong máu kém (là dấu hiệu của suy hô hấp); là biểu hiện của một ca cấp cứu trên lâm sàng và phải đưa vào bệnh viện cấp cứu sớm...

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (5)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (***"how risky is an activity?"***) (***cao hay thấp?)***

  Ví dụ:

  (5) Số CCU (Concurrent Users) chỉ số người sử dụng đồng thời một nguồn tài nguyên số nào đó: RỦI RO không kết nối được vào hệ thống để làm việc hoặc giao dịch.

  KRI = 5 chính là giới hạn (hay ngưỡng) theo giấy phép ('the licensed user limit') số người dùng kết nối đồng thời vào một tài nguyên

  số 1 - 2 - 3 - 4 - **5 – 6 – 7 – 8 – 9 - 10**

  :giá trị càng đến gần lần 5 thì khả năng xảy ra rủi ro (Occ) tăng lên

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (6)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (*"how risky is an activity?"*) (*cao hay thấp?)*

Ví dụ:

(6) Kích thước tải trọng gói tin ("packet's payload size") đo theo MSS: RỦI RO gói tin không đến được nơi nhận do kích thước gói tin lớn hơn MSS và bị mạng "drop".

Metrics (tập số liệu) (byte):

1000 – 1100 – 1200 – 1300 – 1400 - 1460 – 1500

KRI = 1460 byte chính là ngưỡng kích thước tải trọng ('payload') của gói tin.

:giá trị >= 1460 thì khả năng xảy ra rủi ro (Occ) tăng lên

Các ví dụ về chỉ số rủi ro trọng yếu (KRI) (7)

- **KRI là giá trị được sử dụng trong QLRR để nhận ra sự thay đổi mức độ rủi ro của một hoạt động** (***"how risky is an activity?"***) (***cao hay thấp?)***

  Ví dụ:

  (7) Nước nóng: RỦI RO bị bỏng khi tiếp xúc trực tiếp với nước nóng.

  KRI = 56°C chính là giới hạn (hay ngưỡng) nhiệt độ gây bỏng cho da người.

  Metrics (tập số liệu nhiệt độ):

  37°C – 46°C – 56°C – 69°C – 76°C – 86°C - 100°C

  :giá trị càng đến gần sát giá trị 56°C thì mức độ nghiêm trọng của rủi ro (Sev) tăng lên

Các ví dụ khác về chỉ số rủi ro trọng yếu (KRI)

- Hoạt động: Thời gian ngừng hoạt động của thiết bị, mức tồn kho, tỷ lệ luân chuyển nhân viên.
- Tuân thủ: Số phát hiện kiểm toán vi phạm quy định, sự cố vi phạm dữ liệu.
- CNTT: Tính khả dụng của hệ thống, tỷ lệ thời gian ngừng hoạt động của hệ thống hoặc ứng dụng.
- Nguồn nhân lực: Tỷ lệ luân chuyển nhân viên, tình trạng thiếu lao động, tỷ lệ chuyển đổi tuyển dụng thấp.
- Công nghệ: Tính phức tạp của hoạt động, lỗi hệ thống, vấn đề bảo mật.
- Tài chính: Tỷ lệ thanh khoản, tỷ lệ nợ trên vốn chủ sở hữu, mức độ tập trung doanh thu.

Vai trò của chỉ số rủi ro trọng yếu (KRI)

➢ **Vai trò KRI:**

Chỉ số rủi ro trọng yếu (KRI) cung cấp:

- ❑ Giá trị ngưỡng ***("risk threshold")*** chịu đựng rủi ro: là điểm đo lường mà nếu vượt quá thì tổn thất do rủi ro sẽ tăng lên;
- ❑ Mức độ biến thiên/biến đổi của rủi ro: rủi ro đang tăng/giảm (cao/thấp) như thế nào? ***("how risky is it?")***;
- ❑ Phương tiện giám sát từng rủi ro ***("monitor each risk");*** và
- ❑ Công cụ phát hiện và báo hiệu sớm tổn thất do rủi ro đang tăng lên ***("early warning risk" or "early signal of increasing risk exposures")***

Lợi ích của chỉ số rủi ro trọng yếu (KRI)

➢ **Lợi ích của KRI bao gồm:**

• Thông báo (hay dự đoán) trước cho doanh nghiệp về những rủi ro tiềm ẩn có thể gây tổn hại cho doanh nghiệp;

• Tạo ra sự hiểu biết sâu sắc về những điểm yếu có thể có trong các công cụ giám sát và kiểm soát của doanh nghiệp; và

• Giám sát rủi ro liên tục giữa các lần đánh giá rủi ro.

02

Phân biệt KPI và KRI

Phân biệt KPI và KRI(1)

- **Điểm giống nhau:**
  - Các chỉ số (KPI và KRI) được áp dụng cho con người, quy trình, công nghệ, cơ sở vật chất (facilities) và các yếu tố quan trọng khác.
  - Doanh nghiệp sử dụng các chỉ số (KPI và KRI) đánh giá tiến độ hướng tới các mục tiêu đã tuyên bố.

Phân biệt KPI và KRI(2)

- **Điểm khác nhau:**
  - Về chức năng, KPI và KRI là nghịch đảo của nhau.
  - KRI cung cấp các số liệu liên quan đến rủi ro và tác động tiềm tàng của chúng đối với hiệu quả kinh doanh. KRI hoạt động như một khả năng cảnh báo sớm để theo dõi, phân tích, quản lý và giảm thiểu những rủi ro chính.

Phân biệt KPI và KRI(3)

- **Điểm khác nhau:** *(tiếp)*
  - Ngược lại, KPI chứng minh doanh nghiệp đang hoạt động tốt như thế nào so với mục tiêu và mục đích của mình *(ví dụ: doanh số bán hàng, sự hài lòng của khách hàng…);*
  - KPI nhìn lại dữ liệu quá khứ và tập trung vào thành tích mà doanh nghiệp đạt được mục tiêu của mình tốt như thế nào.
  - KPI trả lời câu hỏi *'How well is it?'* / *'How well something is being done'*

Phân biệt KPI và KRI(4)

- **Điểm khác nhau:** *(tiếp)*
  - KRI có tính chất dự đoán. KRI giúp đánh giá và quản lý các rủi ro tiềm ẩn trên lộ trình đạt đến mục tiêu. KRI được liên kết với tình trạng rủi ro và các ưu tiên chiến lược của doanh nghiệp, đồng thời xác định các rủi ro hiện tại và mới nổi liên quan đến từng mục tiêu chính.
  - KRI trả lời câu hỏi *'How risky is it?'* / *'How risky an activity is'*

03

Cách thiết lập và phát triển KRI

Chỉ số rủi ro trọng yếu (KRI)(1)

- Sử dụng KRI giúp doanh nghiệp **dự đoán những rủi ro tiềm ẩn** có thể tác động tiêu cực đến doanh nghiệp. KRI cung cấp một cách để định lượng và giám sát từng rủi ro.
- Hãy xem KRI như những **số liệu liên quan đến thay đổi**, như một hệ thống phát hiện rủi ro cảnh báo sớm để giúp các công ty giám sát, quản lý và giảm thiểu rủi ro một cách hiệu quả.

Chỉ số rủi ro trọng yếu (KRI) (2)

- KRI **cung cấp cái nhìn rõ ràng về những điểm yếu** trong môi trường làm việc và quy trình kiểm soát và rủi ro của doanh nghiệp; đồng thời giúp doanh nghiệp phát triển kế hoạch đánh giá rủi ro để củng cố hoạt động kinh doanh của doanh nghiệp.

Cách thiết lập và phát triển KRI(1)

- Trước khi thiết lập KRI, người thiết lập phải hiểu **mục tiêu** và bất kỳ **điểm yếu** nào có thể gây ra rủi ro cho doanh nghiệp.
- Xác định được nguồn rủi ro (Risk Sources), mối đe dọa và những rủi ro có tác động cao nhất, có khả năng xảy ra cao nhất hoặc có nhiều khả năng nằm ngoài tầm kiểm soát của doanh nghiệp nhất.

Cách thiết lập và phát triển KRI(2)

Nguồn rủi ro ('Risk Source'):

- … **là các yếu tố hoặc thực thể (**mà tự thân nó hoặc trong sự kết hợp**) có thể gây ra (hay khởi tạo) một sự kiện rủi ro** [ISO 31000:2018];
- **… là nguyên nhân gốc rễ của các rủi ro tiềm ẩn;**
- **… là các yếu tố bên ngoài tổ chức như sự biến động của thị trường, thay đổi trong các quy định, thiên tai, thay đổi pháp lý và sự cố công nghệ…;**
- **… các yếu tố bên trong tổ chức như quy trình, nhân sự hoặc dữ liệu…**

Cách thiết lập và phát triển KRI(3)

Xác định nguồn rủi ro sau khi đã biết mục tiêu, mối đe dọa, điểm yếu và rủi ro tiềm ẩn:

- Mục tiêu: Bảo mật 100% tất cả thông tin nhạy cảm;
- Mối đe dọa: Nhân viên CNTT có đặc quyền (là Root/Admin) bất mãn;
- Điểm yếu: Hợp đồng lao động không đãi ngộ tốt người lao động; thông tin nhạy cảm không được bảo vệ và kiểm soát đúng cách;
- Rủi ro tiềm ẩn: Root/Admin có thể tiết lộ thông tin nhạy cảm cho người bên ngoài (*);
- Sự kiện: Giám đốc ra quyết định cho Root/Admin nghỉ việc (sa thải) vào cuối tháng;

>>> Rủi ro (*) đã xảy ra (không còn là tiềm ẩn nữa).

Cách thiết lập và phát triển KRI(4)

>>> **Nguồn rủi ro ('risk source') chính là:**

- **Quyền hạn của Root/Admin; và**
- **Quyết định sa thải nhân sự Root/Admin của Giám đốc.**

Cách thiết lập và phát triển KRI(5)

+ Thiết lập KRI: Tỷ lệ (%) số người biết thông tin nhạy cảm trong doanh nghiệp

+ Ngưỡng giá trị của KRI: i% (ví dụ: 1% - 2%)

Giá trị của ngưỡng giá trị được tính hoặc thay đổi dựa theo:

- Rủi ro tiềm ẩn có thể đã được dự báo;
- Chỉ đạo của cấp lãnh đạo dựa vào Mục tiêu; và
- Quyết định của cấp lãnh đạo (có hay không ra quyết định về một sự kiện)

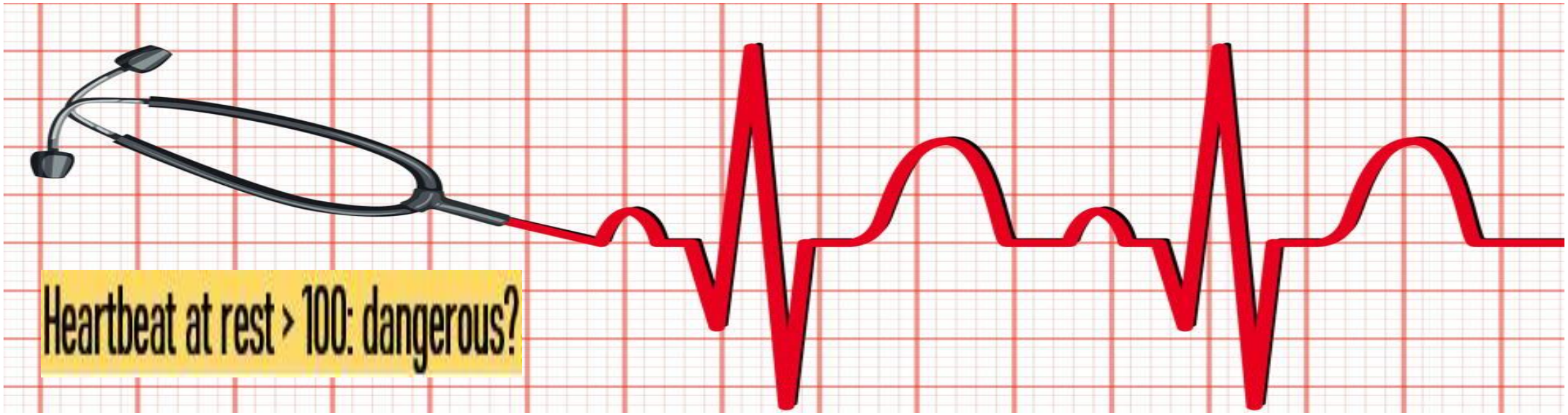
+ Tần suất giảm sát KRI: Hàng tháng vào ngày đầu tiên (hoặc mỗi ngày) theo chính sách ATTT.

Cách thiết lập và phát triển KRI(6)

- Thiết lập KPI trước các KRI tương ứng vì các KPI sẽ cung cấp thông tin cơ bản để có thể lập ra các KRI tương ứng. Khi làm theo cách này, KRI phải phù hợp, kịp thời, có thể đo lường được, có thể dự báo được, có thể so sánh được, dễ hiểu (đối với chủ doanh nghiệp) và là thông tin có ý nghĩa (có ảnh hưởng đến mục tiêu) trong hoạt động của doanh nghiệp.

Cách thiết lập và phát triển KRI(7)

- Thiết lập **ngưỡng giá trị** cho từng KRI đã thiết lập. Nếu giá trị KRI vượt quá ngưỡng này, một hành động phải được thực hiện để bảo vệ mục tiêu *(đáp ứng tiêu chí S.M.A.R.T)* và giảm rủi ro cho doanh nghiệp.



Cách thiết lập và phát triển KRI(8)

- Theo dõi (hoặc giám sát) thường xuyên từng KRI sau khi KRI có hiệu lực thi hành và được áp dụng trong doanh nghiệp.

Cách thiết lập và phát triển KRI(9)

- Xây dựng và sử dụng *"Quy trình thiết lập, đánh giá, giám sát và báo cáo KRI tại doanh nghiệp"* áp dụng khi phải thiết lập KRI.

HOW TO SET UP, EVALUATE, MONITOR AND REPORT KRIs AT THE ENTERPRISE

Step 1	Determine the objectives (targets/goals)
Step 2	Identify threats and weaknesses
Step 3	Identify sources of risk (or risk sources)
…	…
Step n	Set the threshold value of the risk or KRI
…	

Cách thiết lập và phát triển KRI(10)

- Phát triển KRI hiệu quả đòi hỏi phải có:
  - Sự cộng tác và sự tham gia cần thiết của các bên liên quan;
  - Nỗ lực có ý thức, nguồn lực và sự tham gia của người điều hành và các bên liên quan.
  - Nghiên cứu và đánh giá đúng mức độ phức tạp của dữ liệu liên quan đến việc đo lường KRI;
  - Thu thập đủ và thường xuyên dữ liệu, đặc biệt là dữ liệu định lượng về KRI, có thể sử dụng được để đo lường KRI.

Cách thiết lập và phát triển KRI(11)

- Phát triển KRI hiệu quả đòi hỏi phải có: *(tiếp)*
  - Chỉ định người chịu trách nhiệm theo dõi và báo cáo KRI, phát triển các biện pháp ứng phó với rủi ro, cập nhật các biện pháp kiểm soát và đánh giá lại KRI khi có thay đổi quy trình hoặc thay đổi biện pháp kiểm soát, có thay đổi trong bối cảnh hoạt động bên trong hay bên ngoài doanh nghiệp.

04

Các chỉ số rủi ro trọng yếu (KRI) tiêu biểu

Các chỉ số KRI tiêu biểu(1)

➢ **Tại sao chỉ số KRI tiêu biểu lại quan trọng?**

- KRI tiêu biểu là tín hiệu cảnh báo đảm bảo những rủi ro tiềm ẩn được xác định trước và giảm thiểu rủi ro cho doanh nghiệp.
- Nếu không có KRI tiêu biểu, doanh nghiệp (tổ chức) sẽ tăng khả năng gặp phải các sự kiện hoặc tình huống có thể gây thiệt hại đáng kể cho hoạt động kinh doanh của mình.
- KRI tiêu biểu có thể được phân theo 3 nhóm gồm: Người lao động (hay "People"), Quy trình vận hành (hay "Process") và Công nghệ (hay "Technology").

Các chỉ số KRI tiêu biểu(2)

- Thiết lập ngưỡng giá trị cho từng KRI đã thiết lập. Nếu giá trị KRI vượt quá ngưỡng này, một hành động *(đáp ứng tiêu chí S.M.A.R.T)* phải được thực hiện để giảm rủi ro cho doanh nghiệp.
- Ngưỡng giá trị (là giá trị KRI) cho từng doanh nghiệp khác nhau là khác nhau. Giá trị ngưỡng phụ thuộc vào khẩu vị rủi ro ('Risk Appetite') và khả năng chịu đựng rủi ro ('Risk Tolerance') của doanh nghiệp – xem lại định nghĩa ở Chương 01.

Các chỉ số KRI tiêu biểu(3)

- KRI đối với NGƯỜI LAO ĐỘNG / NHÂN VIÊN LÀM VIỆC TẠI DOANH NGHIỆP.
- KRI đối với QUY TRÌNH
- KRI đối với CÔNG NGHỆ

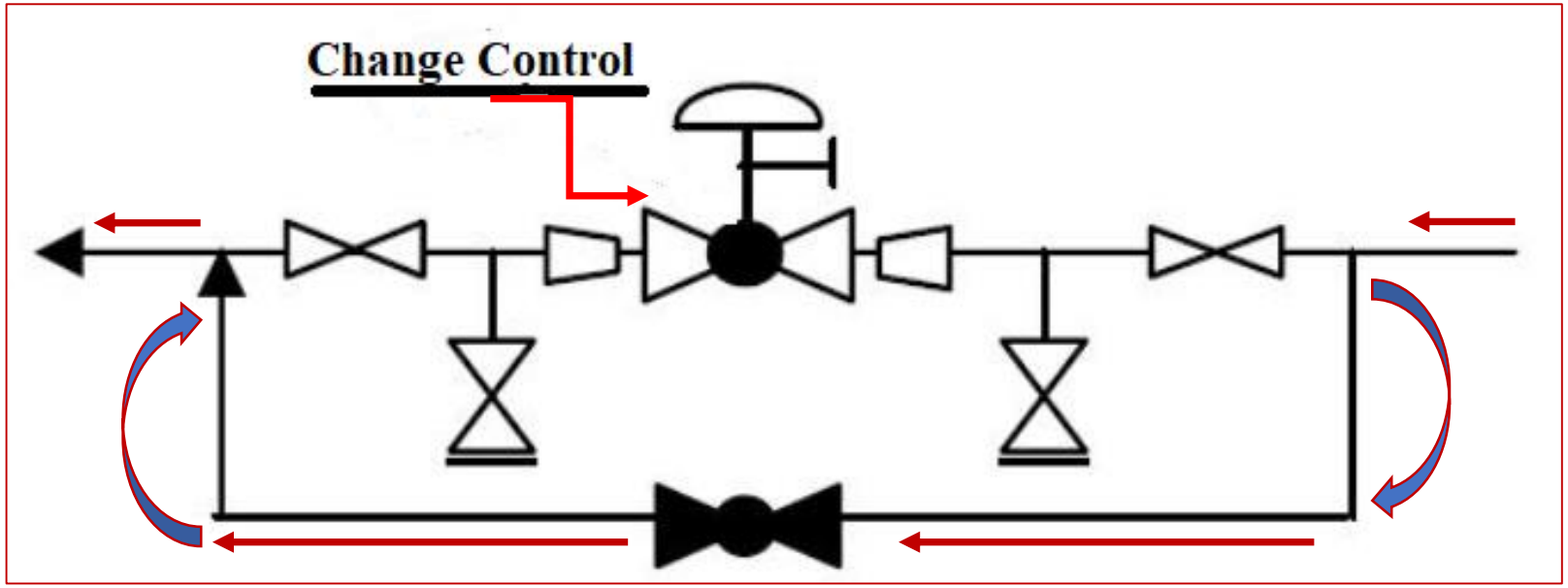
Các chỉ số KRI tiêu biểu – Người lao động(1)

I. Người lao động/Nhân viên:

1. Tỷ lệ nghỉ việc tự nguyện của nhân viên trong mỗi 3 tháng: *Chỉ số này giảm phản ánh mức độ hấp dẫn về môi trường làm việc, chế độ đãi ngộ, văn hóa doanh nghiệp tốt và không ngừng được cải thiện.* Đề nghị KRI <6%.

Các chỉ số KRI tiêu biểu – Người lao động(2)

2. Tỷ lệ % nhân viên bỏ qua hoặc không tuân thủ quy trình kiểm soát sự thay đổi ('Change Control') (A.12.1.2): *Chỉ số này tăng có khả năng tăng rủi ro hoạt động*. Đề nghị KRI = 0%.



Các chỉ số KRI tiêu biểu – Người lao động(2)

3. Tỷ lệ % số lượng khiếu nại liên quan đến công việc của nhân viên hàng tháng: *Chỉ số này tăng giúp nhận ra sự không hài lòng của người lao động đang làm việc tại công ty (tổ chức) tăng lên.*

Đề nghị KRI <15%.

Các chỉ số KRI tiêu biểu – Người lao động(3)

4. Tỷ lệ % người lao động bị xử lý kỷ luật do vi phạm ATTT hàng tháng: *Chỉ số này giảm thể hiện mức độ nhận thức của người lao động về ATTT tăng; thể hiện hình thức xử lý kỷ luật của doanh nghiệp nghiêm khắc như thế nào.* Đề nghị KRI < 1%.

5. Tỷ lệ % lỗi tác nghiệp (cao) còn tồn đọng bị quá hạn khắc phục trong tháng: *Chỉ số này thể hiện năng lực xử lý lỗi của người lao động; mức độ cung cấp nguồn lực/nhân lực để khắc phục; chỉ số hiệu suất công việc của người lao động phù hợp chưa.* Ví dụ: KRI < 0.5%.

Các chỉ số KRI tiêu biểu – Người lao động[4]

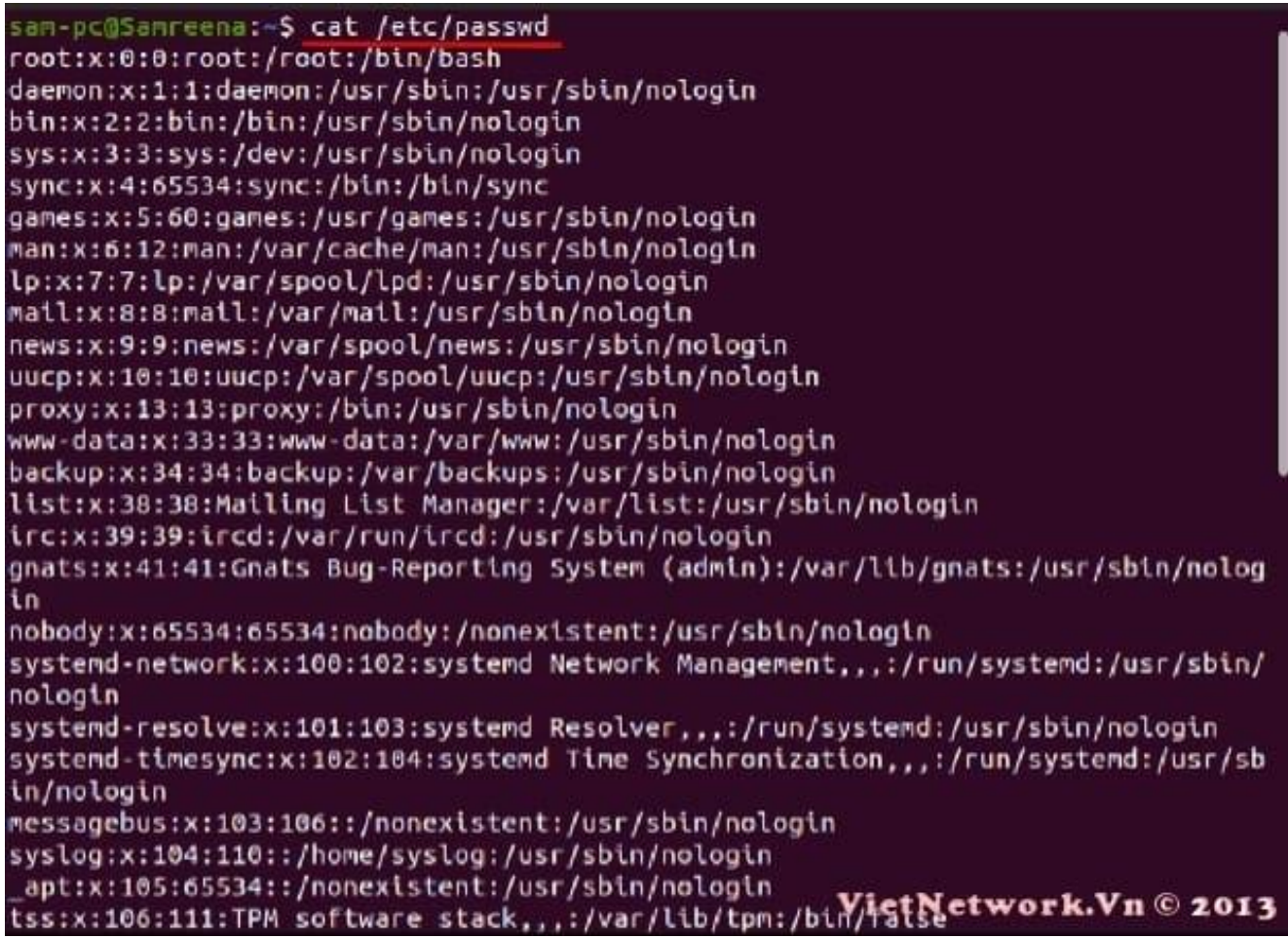
6. Số giờ đào tạo người lao động trong năm: *Chỉ số này thể hiện chất lượng làm việc của người lao động (tốt hay kém); mức độ quan tâm của cấp quản lý đối với thuộc cấp về năng lực chuyên môn (nhiều hay ít).* Ví dụ: KRI >=18 giờ/năm

D	PHÁT TRIỂN CON NGƯỜI		10%												
16	Đào tạo nâng cao năng lực của nhân viên	Số giờ ĐT BQ/NV	5%												
	Số giờ đào tạo cho hệ thống/ năm						≤ 70%	75.0%	80.0%	85.0%	90.0%	95.0%	100.0%	110.0%	115.0%	120.0%
	Số giờ đào tạo bình quân/ nhân viên của đơn vị/ năm						≤18	20	22	24	26	28	30	31	32	33

Xem SoGioDaoTao-1-nam_KPIN2020(duyet).pdf

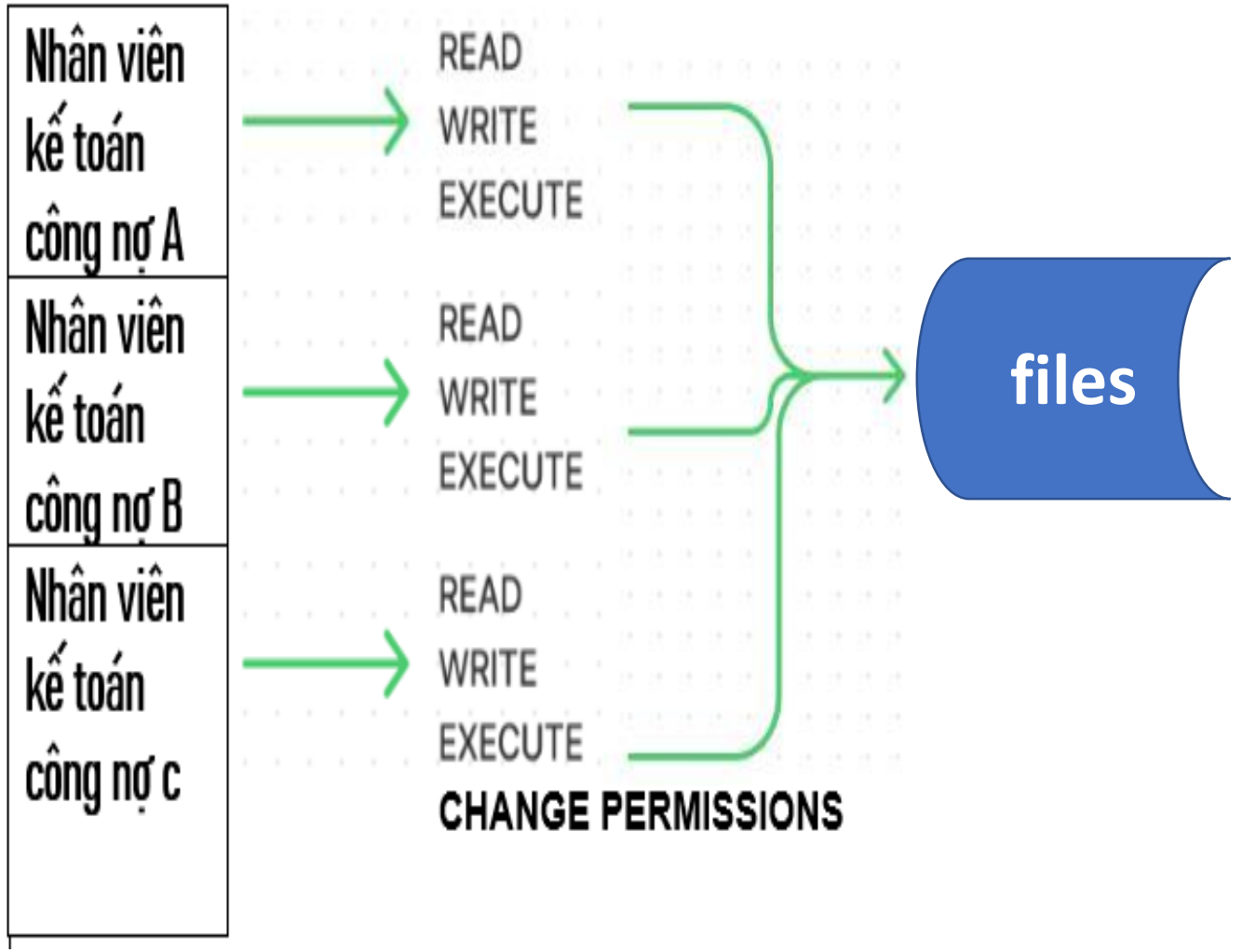
Các chỉ số KRI tiêu biểu – Người lao động(5)

7. Tần suất xem xét các quyền đặc quyền trên hệ thống CNTT trong tháng (A.9.2.3): *chỉ số này tăng thể hiện mức độ quan tâm sự việc có hay không những tài khoản này có khả năng trở thành mục tiêu của kẻ tấn công mạng nhằm giành quyền truy cập vào dữ liệu nhạy cảm.* Đề nghị KRI >= 4.



Các chỉ số KRI tiêu biểu – Người lao động(6)

8. Số lượng người dùng có vai trò tương tự nhưng cách sắp xếp bảo mật khác nhau: *chỉ số này thể hiện khả năng nhân viên có thể đang truy cập dữ liệu khách hàng mà họ không được phép truy cập.* Đề nghị KRI < 1.



Các chỉ số KRI tiêu biểu – Người lao động(7)

9. Tỷ lệ % sự cố bảo mật do lỗi của nhân viên CNTT: *chỉ số này tăng nêu bật các lĩnh vực cần đào tạo, huấn luyện hoặc hỗ trợ thêm.*

Ví dụ: KRI = 1%.

Các chỉ số KRI tiêu biểu – Người lao động(8)

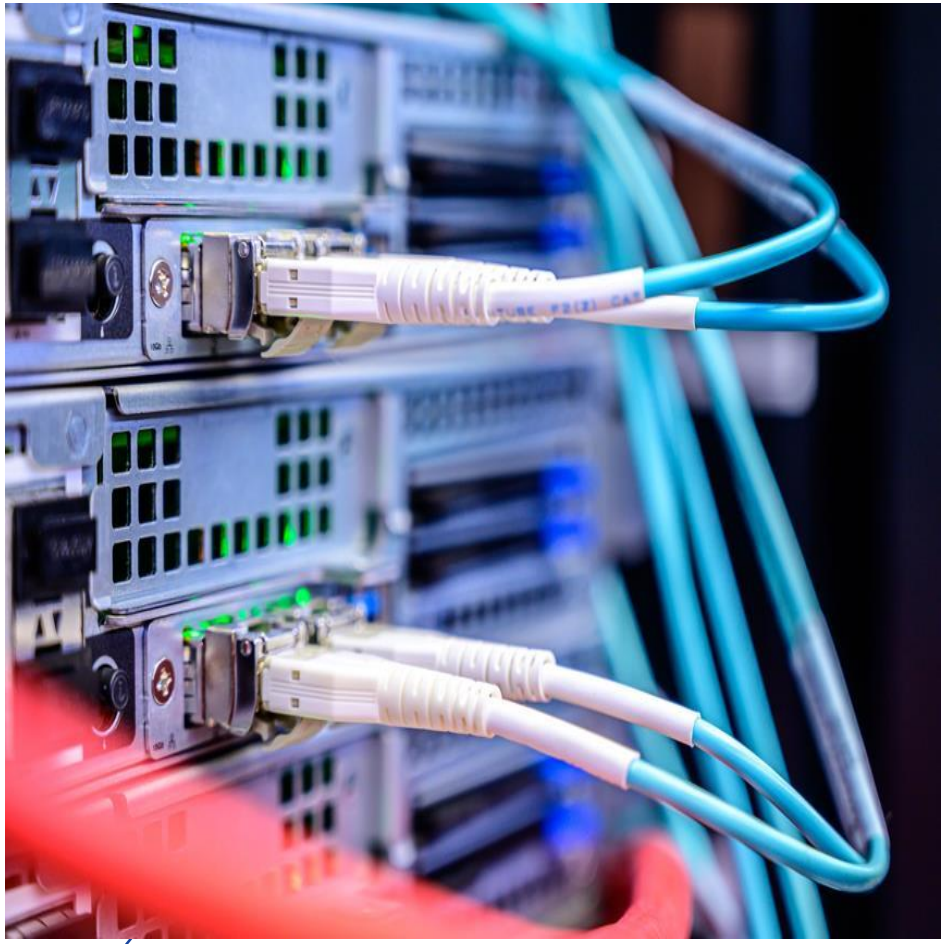
10. Tỷ lệ % nhân viên CNTT có đặc quyền truy cập (A.9.2.3): *chỉ số này tăng làm tăng rủi ro ATTT, vì quyền truy cập quá mức có thể làm tăng nguy cơ bị đe dọa từ nội gián hoặc vi phạm vô tình.*

Ví dụ: KRI = 10%.

Các chỉ số KRI tiêu biểu – Quy trình(1)

II. Vận hành quy trình làm việc

1. Số lượng báo cáo (là tập tin số hóa) gửi qua đường truyền thất bại trong tháng: *Chỉ số này thể hiện lưu lượng (băng thông) không đáp ứng yêu cầu hoạt động; mức độ ổn định hoạt động đường truyền của nhà cung cấp suy giảm; mức độ đáp ứng yêu cầu dự phòng về đường truyền; các biện pháp kiểm soát mạng đáng tin cậy như thế nào (A.13).* Đề nghị KRI < 1.



Các chỉ số KRI tiêu biểu - Quy trình(2)

2. Tỷ lệ cuộc gọi nhỡ phát sinh trong tháng: *Chỉ số này thể hiện mức độ sẵn sàng phục vụ khách hàng của nhân viên quan hệ khách hàng của doanh nghiệp (A.13.1.2; mức độ sao nhãng (hay chểnh mãng) công việc của nhân viên hoặc bị quá tải.*

Ví dụ: KRI < 1%.

Các chỉ số KRI tiêu biểu - Quy trình(3)

3. Số lần nhà cung cấp dịch vụ (điện, hạ tầng mạng WAN, bảo trì máy chủ,…) ngừng hoạt động trong năm: *Chỉ số này thể hiện mức độ sẵn sàng duy trì liên tục dịch vụ cho khách hàng của nhà cung cấp dịch vụ; có hay không thay đổi nhà cung cấp dịch vụ(A.15.2).* Đề nghị KRI < 3.

Các chỉ số KRI tiêu biểu - Quy trình(4)

4. Tỷ lệ của các giao dịch mua bán được duyệt chậm trễ trong ngày: *Chỉ số này thể hiện chỉ số hiệu suất công việc trọng yếu của người lao động phụ trách phê duyệt; thể hiện mức độ đáp ứng với mục tiêu phục vụ khách hàng của doanh nghiệp; người lao động chưa có hoặc chưa cập nhật lại bảng mô tả công việc sao cho phù hợp.(A.7.1.2).*

Ví dụ: KRI < 1%.

Các chỉ số KRI tiêu biểu - Quy trình(5)

5. Số lượng khách hàng khiếu nại về sản phẩm dịch vụ trong tháng:

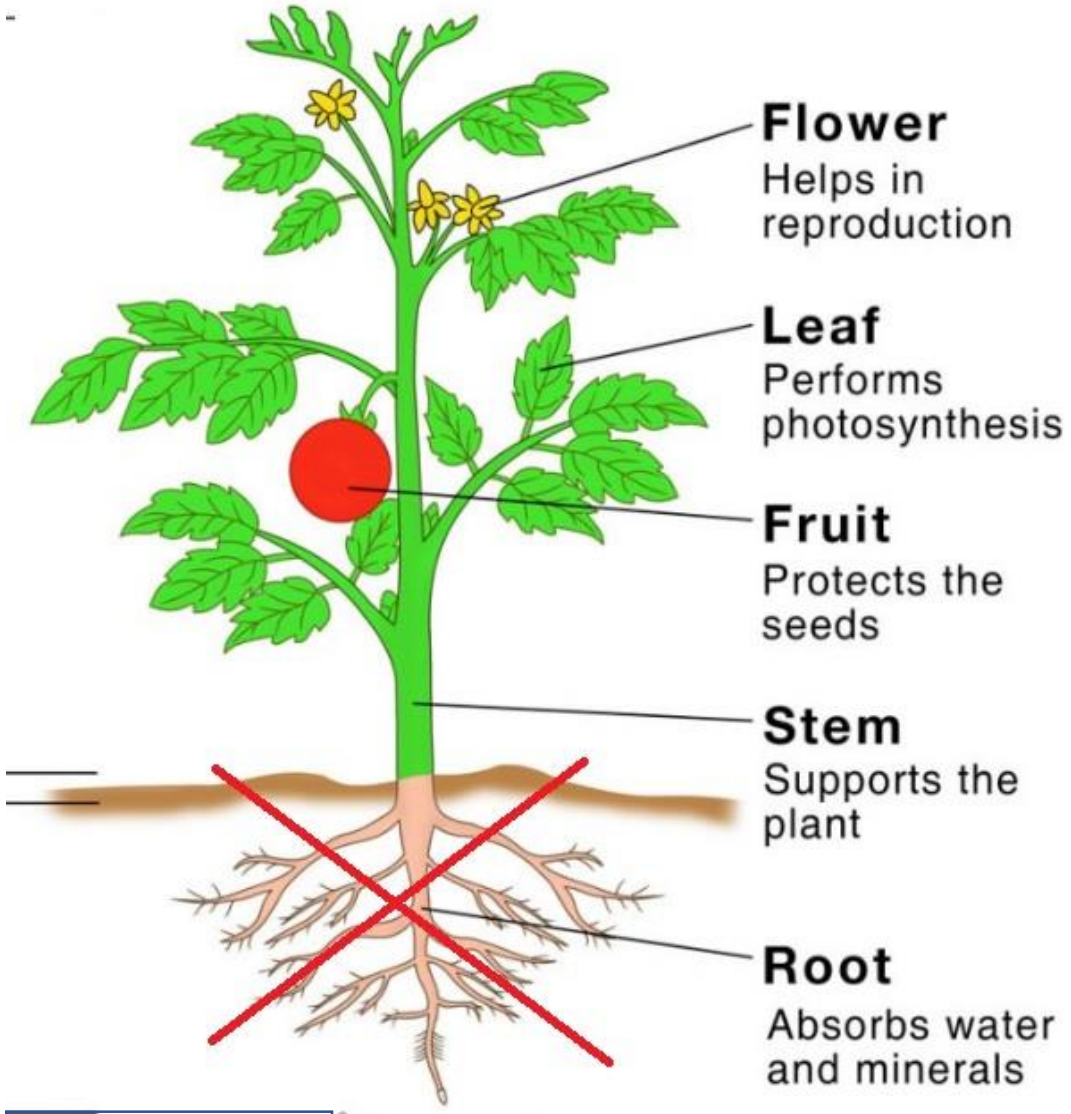
Chỉ số này thể hiện mức độ đáp ứng về tiêu chuẩn chất lượng sản phẩm dịch vụ của doanh nghiệp; có hay chưa có áp dụng bộ tiêu chuẩn quản lý chất lượng.

Ví dụ: KRI < 5

Các chỉ số KRI tiêu biểu - Quy trình(6)

6. Tỷ lệ % các sự cố tương tự tái diễn: *chỉ số này cho thấy nguyên nhân gốc rễ chưa được giải quyết hoặc quy trình ứng phó sự cố không đầy đủ hay có hiệu lực thấp.*

Đề nghị KRI = 0%.



https://greenbiomix.com/

Các chỉ số KRI tiêu biểu - Quy trình(7)

7. Thời gian giải quyết một sự cố nghiêm trọng: c*hỉ số này tăng cao (mất nhiều thời gian hơn) thì quy trình xử lý sự cố nghiêm trọng của doanh nghiệp cần phải rà soát và thay đổi.* Ví dụ: KRI < 60 phút.

Các chỉ số KRI tiêu biểu - Quy trình(8)

8. Số lượng cá nhân giữ tài khoản quản trị: *chỉ số này thể hiện mức độ khó khăn khi chỉ ra ai là thủ phạm khi có rò rỉ dữ liệu (thông tin) xảy ra; việc lạm dụng đặc quyền quản trị có thể xảy ra.*

Ví dụ: KRI < 2.

Các chỉ số KRI tiêu biểu - Quy trình(9)

9. Số lượng hệ thống đồng thời cho phép cùng một tài khoản đăng nhập trong tháng: *chỉ số này thể hiện có hay không nhân viên đã chia sẻ thông tin đăng nhập của họ với các cá nhân trái phép.* Ví dụ: KRI = 0 hệ thống/ tháng.

Các chỉ số KRI tiêu biểu - Quy trình(10)

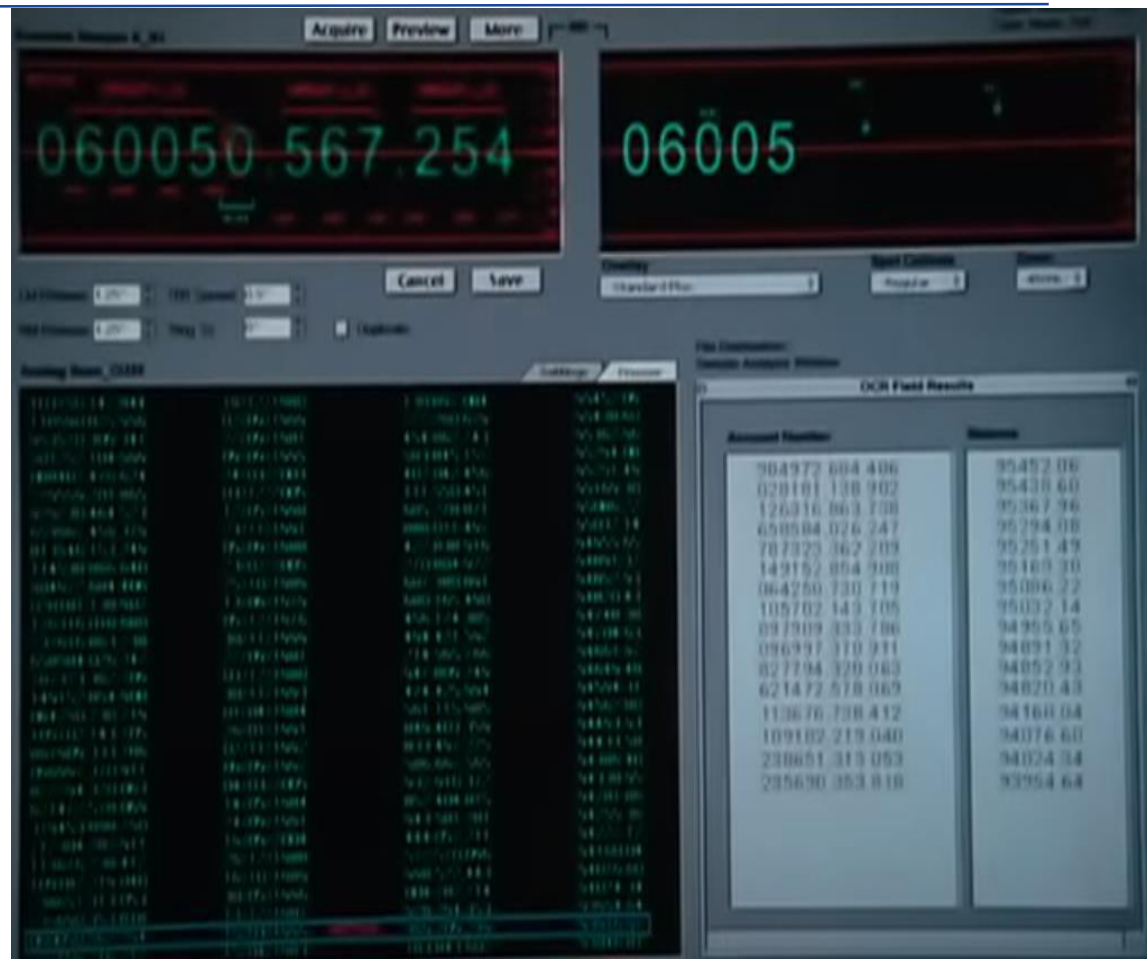
10. Số lần can thiệp thủ công trong tháng để khắc phục lỗi quy trình tự động: *chỉ số này tăng thể hiện lỗi hoặc sự thiếu sót khi thiết kế quy trình tăng.*

Ví dụ: KRI < 1 lần/tháng

Các chỉ số KRI tiêu biểu – Công nghệ(1)

III. Công nghệ

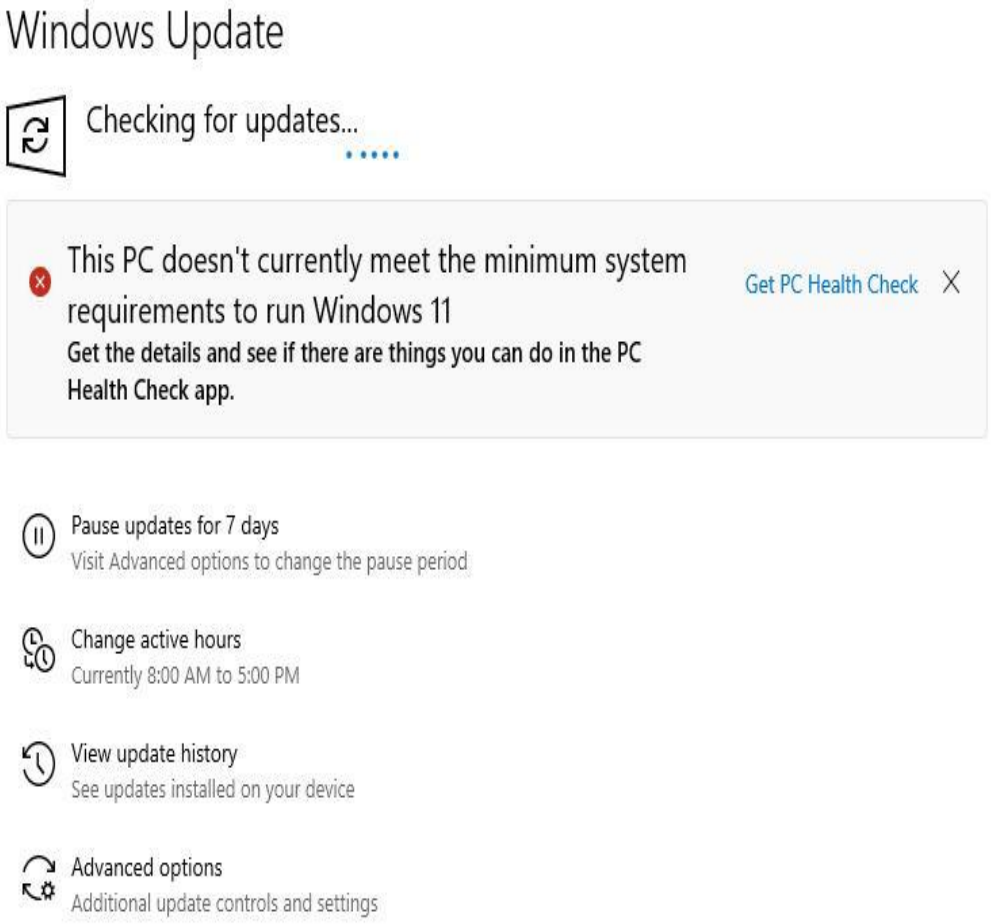
1. Số lần chạy chương trình khóa sổ giao dịch vào cuối ngày (The End of Day routine) bị kéo dài trong tháng làm ảnh hưởng đến vận hành ngày hôm sau: *Chỉ số này thể hiện hiệu suất làm việc của hệ thống / ứng dụng CNTT của doanh nghiệp; mức độ quá tải của hệ thống/ứng dụng.(A.12, A.12.1.3)*



Ví dụ: KRI < 2 lần/tháng

Các chỉ số KRI tiêu biểu – Công nghệ(2)

2. Triển khai bản vá lỗi (Patches) an ninh mạng trong tháng cho hệ thống chậm hơn 1/2/3/… bản vá (patches) so với mức dự kiến và/hoặc so với khuyến nghị: *chỉ số này giúp xác định mức độ vá lỗi tối ưu cho hệ thống an ninh mạng (không trễ hơn bao nhiêu bản vá hoặc không trễ hơn bao nhiêu ngày so với yêu cầu của nhà cung cấp)(A.12.2, A.14.2).*



Ví dụ: KRI < 2/tháng

Các chỉ số KRI tiêu biểu – Công nghệ(3)

3. Hệ thống sao lưu gửi cảnh báo khi mức độ dự phòng giảm xuống dưới khung thời gian tối thiểu có thể chấp nhận được: *chỉ số này chứng minh rằng tài sản CNTT đang ở mức dự phòng mới nhất là bao nhiêu và nếu xảy ra sự cố hệ thống thì khả năng phục hồi dữ liệu là bao nhiêu (A.12.3).*

Ví dụ: KRI > 24 giờ

Các chỉ số KRI tiêu biểu – Công nghệ(4)

4. Mức độ sẵn sàng trong tháng của các hệ thống/ứng dụng CNTT trọng yếu: *Chỉ số này thể hiện khả năng đảm bảo hoạt động liên tục của hệ thống (A.17, A.17.2) và mức đáp ứng yêu cầu dự phòng.*

Ví dụ: KRI > = 99.72%

Các chỉ số KRI tiêu biểu – Công nghệ(5)

5. Số lượng trường hợp xảy ra gián đoạn hệ thống giao dịch do mã độc (malware, virus…) trong tháng (năm): *Chỉ số này thể hiện tính liên tục của ATTT tại doanh nghiệp chưa được đưa vào hệ thống quản lý tính liên tục (BCP); mức độ hiệu quả kịch bản xử lý sự cố. (A.17.1, A.17.2).*

Ví dụ KRI <= 2 (lần/tháng)

Các chỉ số KRI tiêu biểu – Công nghệ(6)

6. Khi xảy ra sự cố mất điện lưới, thời gian duy trì hoạt động của hệ thống máy tính tại doanh nghiệp bằng nguồn dự phòng (qua UPS) không dưới ngưỡng thời gian tối thiểu: *chỉ số này thể hiện khả năng mất dữ liệu xảy ra (có hay không, nhiều hay ít) khi mất nguồn điện chính (điện lưới).*

Ví dụ: KRI >= 15 phút

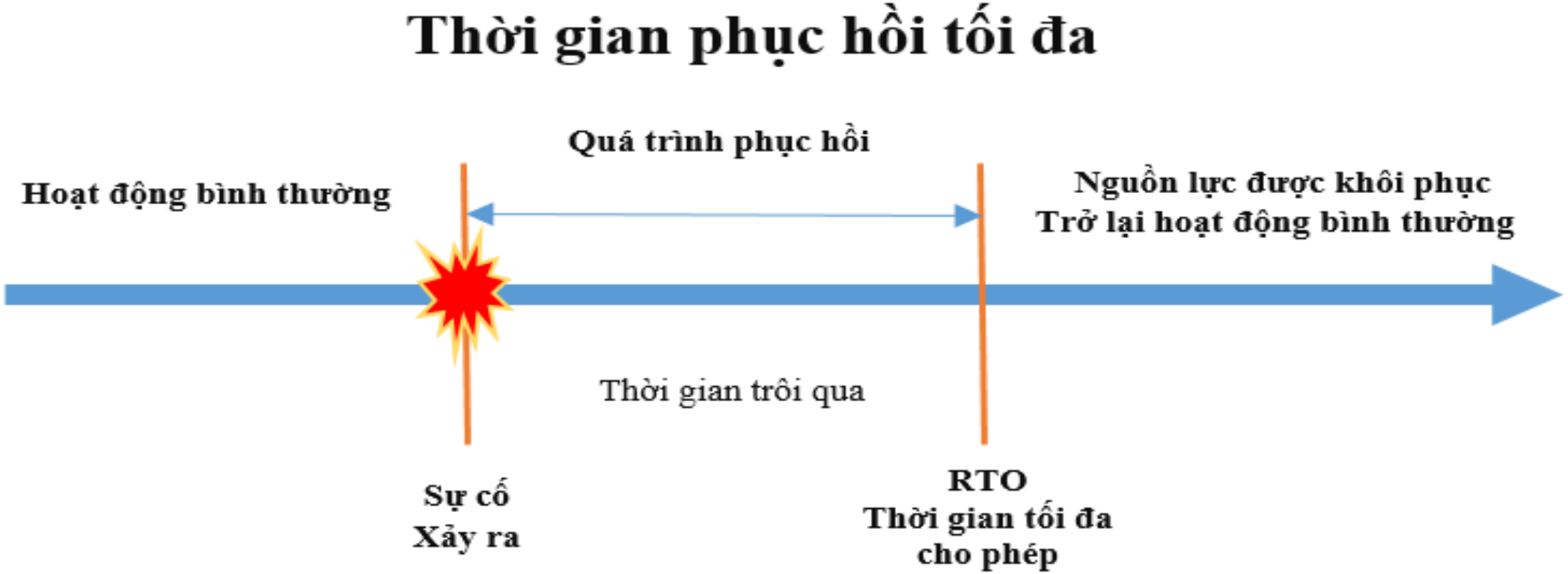
Các chỉ số KRI tiêu biểu – Công nghệ(7)

7. Thời gian tối đa có thể chấp nhận được (hay cho phép) (là chỉ số RTO – Recovery Time Objective) mà máy tính, hệ thống, mạng hoặc ứng dụng có thể ngừng hoạt động sau khi xảy ra lỗi hoặc thảm họa: *chỉ số này thể hiện năng lực xử lý (nhanh hay tốt như thế nào) rủi ro gây gián đoạn hoạt động của doanh nghiệp.*

Ví dụ: KRI <= 120 phút

Các chỉ số KRI tiêu biểu – Công nghệ(8)

Thời gian tối đa có thể chấp nhận được (hay cho phép) (là chỉ số RTO – Recovery Time Objective) ….*(tiếp)*



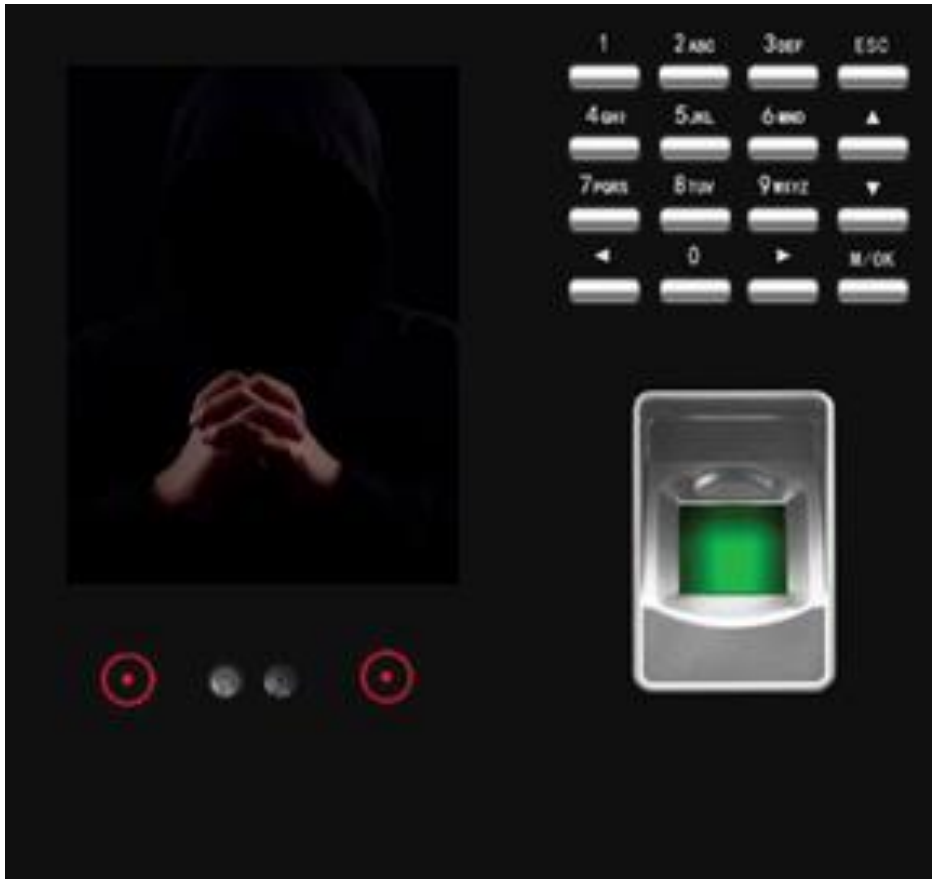
Các chỉ số KRI tiêu biểu – Công nghệ(9)

8. Thời gian nhân viên HelpDesk giải quyết xong một yêu cầu của một người sử dụng (Normal User) trong tháng: *chỉ số này thể hiện năng lực làm việc và kiến thức của nhân viên kỹ thuật (hệ thống/mạng/ứng dụng/ cung ứng dịch vụ/…) thuộc bộ phận HelpDesk của doanh nghiệp; mức độ sẵn sàng làm việc.* Ví dụ: KRI <= 10 phút

Các chỉ số KRI tiêu biểu – Công nghệ(10)

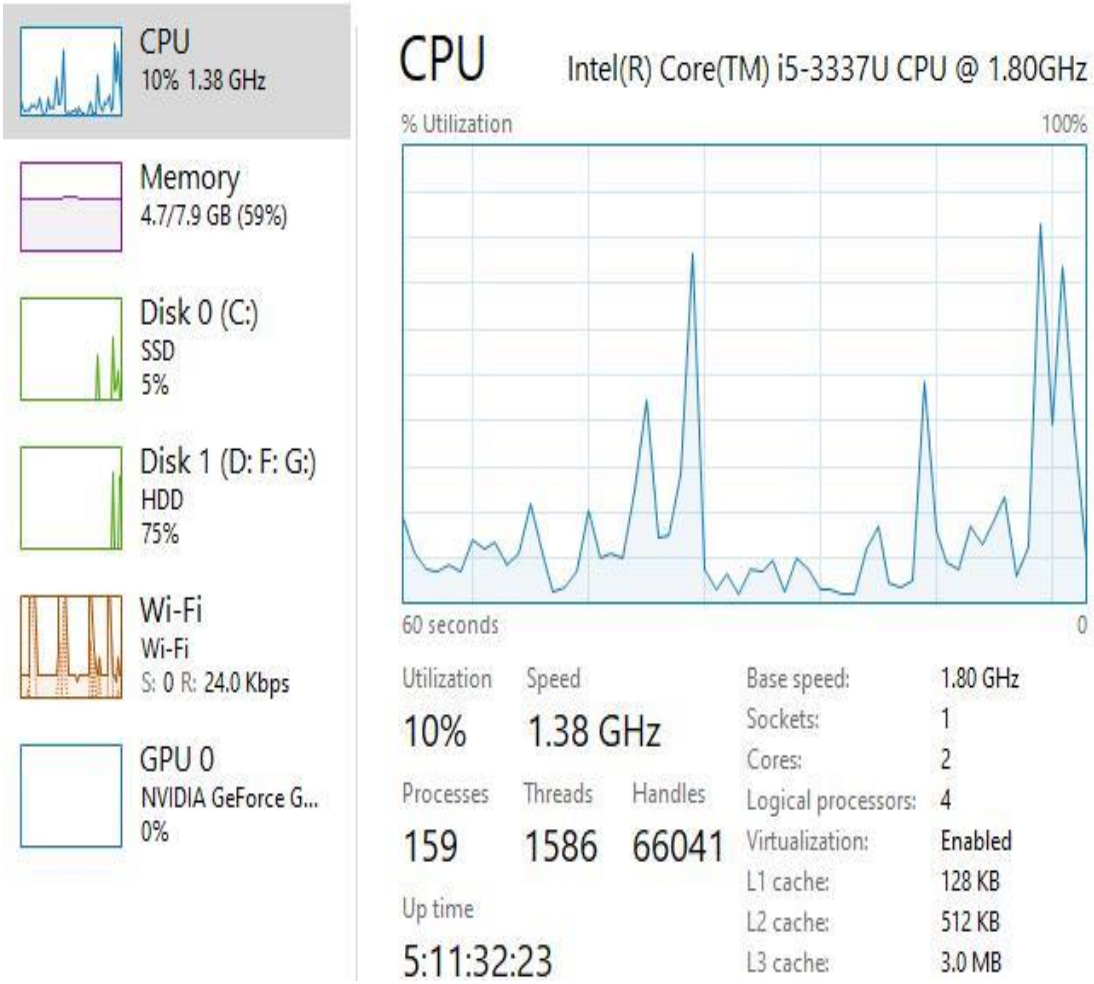
9. Tần suất các lần đăng nhập không thành công và/hoặc truy cập trái phép vào hệ thống/ứng dụng trong tháng: *chỉ số này thể hiện các mối đe dọa bảo mật tiềm ẩn và/hoặc hành vi (hay đặc điểm, cá tính) của người dùng.*

Ví dụ: KRI = 5 lần/tháng



Các chỉ số KRI tiêu biểu – Công nghệ(11)

10. Theo dõi năng lực hệ thống để dự đoán khi nào tài nguyên có thể cạn kiệt và chủ động giải quyết các tắc nghẽn tiềm ẩn: *chỉ số này thể hiện yêu cầu phải tăng năng lực xử lý (%) trong tương lai khi lập kế hoạch hàng năm đầu tư nâng cao năng lực (ví dụ trang bị SAN/NAS, bộ vi xử lý mới, RAM, HDD,…).* Ví dụ KRI = 25%



Hết Chương 9

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/, https://look.s3.com.tw/ , https://enggcyclopedia.com/