BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 2029/QĐ-BTTTT	*Hà Nội, ngày 23 tháng 10 năm 2023*

QUYẾT ĐỊNH

Ban hành "Mô hình đánh giá mức độ trưởng thành của đội ứng cứu sự cố an toàn thông tin mạng"

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 48/2022/NĐ-CP ngày 26 tháng 07 năm 2022 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng tại Việt Nam;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Mô hình đánh giá mức độ trưởng thành của đội ứng cứu sự cố an toàn thông tin mạng" (sau đây gọi tắt là "Mô hình đánh giá").

Điều 2. Mô hình đánh giá là công cụ để thực hiện khảo sát, đánh giá mức độ trưởng thành của đội ứng cứu sự cố an toàn thông tin mạng tại Việt Nam theo từng giai đoạn; đồng thời là bộ tài liệu hướng dẫn hoạt động về ứng cứu sự cố an toàn thông tin mạng cho các thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và các đội ứng cứu sự cố an toàn thông tin mạng có liên quan khác.

Điều 3. Giao Cục An toàn thông tin xây dựng và ban hành tài liệu hướng dẫn; chủ trì, phối hợp với các cơ quan, tổ chức liên quan tổ chức triển khai, áp

dụng, đánh giá, công bố kết quả đánh giá đối với các thành viên Mạng lưới Ứng cứu sự cố an toàn thông tin mạng quốc gia và các đơn vị liên quan khác theo Mô hình này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Huy Dũng;
- Cổng thông tin điện tử của Bộ TT&TT;
- Các đơn vị chuyên trách về CNTT/ATTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Lưu: VT, CATTT.VNCERT/CC BTH.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Huy Dũng

MÔ HÌNH ĐÁNH GIÁ MỨC ĐỘ TRƯỞNG THÀNH CỦA ĐỘI ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Kèm theo Quyết định số 3029/QĐ-BTTTT ngày 25/10/2023 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Mục đích ban hành

Sự trưởng thành của đội ứng cứu sự cố an toàn thông tin mạng (gọi tắt là CSIRT) là cách gọi thể hiện mức độ phát triển của CSIRT khi triển khai đồng bộ các công tác tổ chức, quản trị, xây dựng hồ sơ, văn bản, tài liệu, hoạt động thực thi và đo lường chức năng, nhiệm vụ của CSIRT đó.

Tại Việt Nam hiện chưa có tài liệu hướng dẫn, thiếu công cụ đánh giá để giúp các tổ chức có định hướng phát triển và tổ chức hiệu quả hoạt động của CSIRT một cách toàn diện. "Mô hình đánh giá mức độ trưởng thành của CSIRT" (sau đây gọi tắt là "Mô hình" hoặc "Mô hình đánh giá") được xây dựng nhằm mục đích giải quyết vấn đề nêu trên, giúp các tổ chức đánh giá đúng thực trạng hiện tại của CSIRT và xác định được những việc cần làm, các khuôn khổ, nền tảng cần xây dựng để đạt được mục tiêu đề ra theo các mức độ trưởng thành.

Mô hình đánh giá này cũng là một tài liệu hướng dẫn cho các CSIRT triển khai các hoạt động theo quy định của Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; theo Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng tại Việt Nam; và Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng.

Việc đánh giá CSIRT sẽ được triển khai theo 3 giai đoạn chính ***(phụ lục kèm theo)***. Tùy vào năng lực CSIRT hiện tại, các cơ quan, tổ chức lựa chọn giai đoạn phù hợp để bắt đầu áp dụng. Tuy nhiên, khuyến khích các cơ quan, tổ chức nên lựa chọn giai đoạn 3 để thực hiện xuyên suốt việc đánh giá mức độ trưởng thành đội ứng cứu sự cố an toàn thông tin mạng.

2. Phạm vi áp dụng

Tài liệu này có thể áp dụng cho tất cả các đội ứng cứu sự cố an toàn thông tin mạng tại Việt Nam. Các chỉ số đánh giá mức độ trưởng thành của CSIRT trong tài liệu đề cập toàn diện về mô hình tổ chức và phương pháp thực hiện đảm bảo an toàn thông tin mạng, bao gồm các nhóm chỉ số: chỉ số về tổ chức, chỉ số về con người, chỉ số về công cụ, chỉ số về quy trình và chỉ số về hoạt động thường xuyên.

3. Đối tượng áp dụng

Mô hình đánh giá này áp dụng đối với các cơ quan, tổ chức, doanh nghiệp là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, đồng thời khuyến khích các tổ chức thực hiện ứng cứu sự cố an toàn thông tin mạng khác tham khảo áp dụng.

4. Từ viết tắt:

- VNCERT/CC: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam trực thuộc Cục An toàn thông tin (Bộ Thông tin và Truyền thông).
- CSIRT: Đội ứng cứu sự cố an toàn thông tin mạng.
- Mạng lưới: Mạng lưới Ứng cứu sự cố an toàn thông tin mạng quốc gia.
- Cơ quan điều phối quốc gia: Cơ quan điều phối quốc gia về ứng cứu sự cố an toàn thông tin mạng.
- CNTT: công nghệ thông tin.
- VNO: chỉ số về tổ chức.
- VNH: chỉ số về con người.
- VNT: chỉ số về công cụ.
- VNP: chỉ số về quy trình.
- VNA: chỉ số về hoạt động thường xuyên.

II. MÔ HÌNH ĐÁNH GIÁ VÀ PHƯƠNG PHÁP ĐÁNH GIÁ

1. Danh sách các chỉ số đánh giá :

Mô hình đánh giá mức độ trưởng thành của đội ứng cứu sự cố bao gồm 05 nhóm chỉ số lớn với 44 chỉ số thành phần, cụ thể như sau:

STT	Tên chỉ số	Tên ký hiệu
I	**Nhóm chỉ số đánh giá về tổ chức**	**VNO**
1	Chức năng, nhiệm vụ	VNO-1

2	Đối tượng phục vụ	VNO-2
3	Quyền hạn	VNO-3
4	Trách nhiệm	VNO-4
5	Danh mục các hoạt động nghiệp vụ	VNO-5
6	Phân loại sự cố	VNO-6
7	Quy chế hoạt động	VNO-7
8	Chính sách bảo mật	VNO-8
II	**Nhóm chỉ số đánh giá về con người**	**VNH**
9	Quy tắc ứng xử	VNH-1
10	Phương án dự phòng nhân sự	VNH-2
11	Yêu cầu về kỹ năng	VNH-3
12	Phát triển đội ngũ	VNH-4
13	Đào tạo kỹ thuật	VNH-5
14	Đào tạo kỹ năng mềm	VNH-6
15	Kết nối- hợp tác	VNH-7
III	**Nhóm chỉ số đánh giá về công cụ**	**VNT**
16	Danh sách tài nguyên CNTT	VNT-1
17	Danh sách nguồn thông tin	VNT-2
18	Kênh thông tin liên lạc không gián đoạn	VNT-3
19	Hệ thống theo dõi sự cố	VNT-4
20	Đảm bảo kết nối internet ổn định	VNT-5
21	Bộ công cụ phòng ngừa sự cố	VNT-6
22	Bộ công cụ phát hiện sự cố	VNT-7
23	Hệ thống xử lý sự cố	VNT-8
IV	**Nhóm chỉ số đánh giá về quy trình**	**VNP**

24	Quy trình báo cáo sự cố lên cấp quản lý cao hơn	VNP-1
25	Quy trình công khai thông tin	VNP-2
26	Quy trình cung cấp thông tin cho cơ quan pháp lý	VNP-3
27	Quy trình phòng ngừa sự cố	VNP-4
28	Quy trình phát hiện sự cố	VNP-5
29	Quy trình xử lý sự cố	VNP-6
30	Quy trình đánh giá hoàn thiện tổ chức	VNP-7
31	Quy trình tiếp cận khẩn cấp	VNP-8
32	Quy trình xử lý thông tin mật	VNP-9
33	Quy trình quản lý nguồn tin	VNP-10
34	Quy trình tiếp cận khách hàng, đối tác	VNP-11
35	Quy trình kết nối cơ quan quản lý nhà nước	VNP-12
36	Quy trình thống kê sự cố	VNP-13
37	Quy trình họp	VNP-14
38	Quy trình phối hợp trong Mạng lưới	VNP-15
V	**Nhóm chỉ số đánh giá hoạt động thường xuyên**	**VNA**
39	Kế hoạch hoạt động	VNA-1
40	Tham gia nền tảng IRLab	VNA-2
41	Rà quét lỗ hổng	VNA-3
42	Săn lùng mối nguy	VNA-4
43	Diễn tập thực chiến	VNA-5
44	Chia sẻ thông tin	VNA-6

2. Thang điểm và phương pháp đánh giá

2.1. Thang điểm

Mỗi chỉ số đều có 5 mức đánh giá và số điểm được cho tương ứng với các mức này. Bảng điểm cụ thể được ghi rõ ở mỗi chỉ số.

Các điểm được tính từ 0 đến 4, qua mỗi điểm tăng lên thể hiện từng bước trưởng thành của CSIRT bằng các hành động cụ thể. Đó là:

Mức 1 là điểm "0" dành cho CSIRT hoàn toàn không có khái niệm gì về các hoạt động được nêu trong chỉ số đưa ra, chưa ai thảo luận về hoạt động này.

Mức 2 là điểm "1" dành cho CSIRT đã có bước tiến về nhận thức, đã biết về hoạt động, có thể đã thực hiện thực tế, nhưng hoạt động này chưa được ghi lại thành văn bản, do đó, không có chứng cứ để chứng minh cho việc đã nhận thức hay đã làm này.

Mức 3 là điểm "2" dành cho CSIRT đã có hoạt động và đã ghi chép lại thành tài liệu, nhưng đây mới là hành động tự phát, hoặc mới trong giai đoạn dự thảo, chưa được phê duyệt.

Mức 4 là điểm "3" dành cho CSIRT đã bắt đầu hoạt động chuyên nghiệp khi đã triển khai hoạt động, có xây dựng tài liệu chính thức, thành các quy định, quy trình vận hành của tổ chức và đã được lãnh đạo phê duyệt.

Mức 5 là điểm "4" dành cho CSIRT đã vận hành tốt, hoạt động được lập thành tài liệu chính thức, được phê duyệt, được công bố. Và CSIRT đã đạt đến bước có hoạt động đánh giá định kỳ để thực hiện cải tiến và phát triển.

2.2. Các mức độ trưởng thành

Thang điểm đánh giá tổng thể về mức độ trưởng thành của CSIRT trong Mô hình này có 5 mức: Ý tưởng (E), Sơ khởi (D), Cơ bản (C), Hoàn thiện (B), Tối ưu (A).

Chi tiết thang điểm đánh giá các mức độ trưởng thành CSIRT được trình bày cụ thể như sau:

Mức độ trưởng thành	Tên các giai đoạn	Số điểm	Đặc điểm

A	Tối ưu	> 132	CSIRT phát triển toàn diện về tổ chức, nhân sự chất lượng, công cụ được trang bị đầy đủ, quy trình thường xuyên được xem xét, cập nhật để đánh giá tính hiệu quả. CSIRT luôn được cải tiến theo chu kỳ, đảm bảo năng lực phát hiện, cảnh báo, phân tích, xử lý sự cố và phục hồi hệ thống. Các bài học kinh nghiệm của CSIRT được ghi lại và chia sẻ trong toàn Mạng lưới.
B	Hoàn thiện	107 -132	CSIRT bắt đầu đi vào hoạt động bài bản. Ngoài các mức trưởng thành như mức độ C, CSIRT bắt đầu thiết lập các chức năng quản lý sự cố, đồng thời triển khai một số hoạt động thường xuyên để nâng cao năng lực CSIRT.
C	Cơ bản	71 -106	CSIRT đạt mức trưởng thành cơ bản, có sự phân chia nhiệm vụ và phạm vi hoạt động, bắt đầu có quy trình xử lý sự cố và thực hiện việc phối hợp xử lý các sự cố ở mức cơ bản.
D	Sơ khởi	33-70	CSIRT đang trong quá trình hình thành. CSIRT có đầu mối liên hệ (PoC) tiếp nhận và gửi thông tin sự cố, có các quy tắc và quy định để thông báo cho các đơn vị có liên quan về việc này.
E	Ý tưởng	<33	CSIRT giai đoạn đầu tiên. Công việc của các tổ chức đòi hỏi có đội ngũ đảm nhận trách nhiệm ứng cứu sự cố an toàn thông tin mạng và vấn đề thành lập CSIRT bắt đầu được nhắc đến.

2.3. Phương pháp đánh giá

Khi thực hiện đánh giá một CSIRT, mỗi chỉ số được cho số điểm tương ứng. Số điểm này được dùng để sơ đồ hóa cho thấy mô hình và mức độ phát

triển từng mặt cụ thể của CSIRT.

Cục An toàn thông tin, Bộ Thông tin và Truyền thông xây dựng nền tảng mở dành cho các CSIRT tự đánh giá theo 3 phần hiển thị gồm: (1) Biểu đồ mạng nhện/Hiển thị câu hỏi giúp so sánh kết quả từ các câu hỏi khác nhau và trực quan hóa phần hiển thị kết quả bằng hình đồ họa; (2) Bảng kết quả liệt kê đầy đủ các điểm số của từng chỉ số và có đánh giá ngắn gọn về mức độ đạt yêu cầu hay không với mỗi chỉ số; và (3) Tư vấn mở cho biết các chỉ số nào cần được cải thiện và các hành động cụ thể cần thực hiện.

Quá trình triển khai đánh giá mức độ trưởng thành của các đội CSIRT được triển khai như sau:

- Cục An toàn thông tin đưa ra bảng điều tra khảo sát (mỗi giai đoạn triển khai sẽ có các bảng điều tra tương ứng) bao gồm các câu hỏi cụ thể theo từng chỉ số và gửi cho các thành viên Mạng lưới, muộn nhất vào ngày 25/7 hàng năm.

- Các đơn vị được đánh giá trả lời các câu hỏi trong bảng câu hỏi, kèm theo các tài liệu chứng minh và gửi về Cục An toàn thông tin, muộn nhất vào ngày 25 tháng 9 hàng năm.

- Cục An toàn thông tin xác minh, kiểm chứng thông tin trả lời của các đơn vị và đưa ra kết luận đánh giá, muộn nhất vào ngày 25 tháng 11 hàng năm.

- Cục An toàn thông tin thực hiện báo cáo Bộ Thông tin và Truyền thông và đưa ra thông báo công khai kết quả đánh giá, xếp hạng các đơn vị muộn nhất vào ngày 25 tháng 12 hàng năm.

Ưu tiên phương án điều tra khảo sát, trả lời câu hỏi, xác minh, kiểm chứng thông tin, đánh giá, xếp hạng thông qua phương pháp trực tuyến trên nền tảng số do Cục An toàn thông tin triển khai.

3. Nội dung các chỉ số và bảng điểm đánh giá cụ thể

3.1. Nhóm chỉ số đánh giá về tổ chức (Organization)

VNO-1: Chức năng, nhiệm vụ

Trong đảm bảo an toàn thông tin mạng, đội ứng cứu sự cố an toàn thông tin mạng (CSIRT) có vai trò là lực lượng nòng cốt triển khai các biện pháp

phòng và chống các tấn công mạng. Các tổ chức cần xây dựng và phát triển lực lượng này. Để CSIRT hoạt động hiệu quả, bộ máy tổ chức của CSIRT cần được tổ chức bài bản và chuyên nghiệp, có chức năng, nhiệm vụ rõ ràng, cụ thể.

Điểm đánh giá:

0: Chưa hình thành đội/ nhóm ứng cứu sự cố (CSIRT) trong tổ chức. Các nhiệm vụ đảm bảo an toàn thông tin chưa tách riêng với nhiệm vụ công nghệ thông tin,

1: Chưa hình thành đội/ nhóm ứng cứu sự cố trong tổ chức, nhưng nhiệm vụ đảm bảo an toàn thông tin đã có các hoạt động được triển khai riêng. Tùy từng nhiệm vụ, lãnh đạo tổ chức giao cho những người khác nhau triển khai.

2: Đội ứng cứu sự cố chưa có quyết định thành lập chính thức, nhưng đã bắt đầu làm việc theo nhóm trong các hoạt động liên quan.

3: Đã có quyết định thành lập đội ứng cứu sự cố, có phân công nhiệm vụ rõ ràng, tuy nhiên tất cả đều là các thành viên kiêm nhiệm.

4: CSIRT đã có quyết định thành lập, có chức năng, nhiệm vụ rõ ràng, có thành viên chuyên trách.

VNO-2: Đối tượng phục vụ

Một CSIRT có thể chỉ chịu trách nhiệm ứng cứu sự cố an toàn thông tin mạng cho nội bộ tổ chức, hoặc có thể đảm bảo an toàn thông tin cho các cá nhân, tổ chức bên ngoài; như bảo vệ hệ thống thông tin cho các cơ quan chính phủ, hoặc cung cấp các dịch vụ thương mại về ứng cứu sự cố cho cộng đồng.

Các cá nhân, tổ chức, các hệ thống, thiết bị mà CSIRT có trách nhiệm, có cam kết hỗ trợ, có cung cấp dịch vụ ứng cứu sự cố đó được gọi là "đối tượng phục vụ". Một CSIRT hoạt động phải xác định rõ các đối tượng phục vụ.

Điểm đánh giá:

0: Các thành viên CSIRT không xác định được đối tượng phục vụ của mình.

1: Các thành viên của CSIRT biết đối tượng phục vụ của đội mình, nhưng chưa có văn bản nào thể hiện điều này.

2: Các thành viên của CSIRT đã dự thảo văn bản đề cập đến đối tượng phục vụ của đội mình, nhưng chưa được cấp trên phê duyệt.

3: CSIRT đã có văn bản chính thức quy định rõ các đối tượng phục vụ.

4: CSIRT đã có văn bản chính thức quy định rõ các đối tượng phục vụ. Trong quá trình triển khai, các thành viên của CSIRT luôn có đánh giá định kỳ, kiểm tra để điều chỉnh khi cần.

VNO-3: Quyền hạn

CSIRT phải có quyền hạn nhất định để CSIRT hoạt động và phát triển. Tùy theo chức năng, nhiệm vụ, đối tượng, phạm vi, lĩnh vực của CSIRT mà quyền hạn đó được các cấp quản lý cao hơn quy định phù hợp.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết về quyền hạn của mình.

1: Các thành viên của CSIRT biết quyền hạn của mình, nhưng chưa nhìn thấy văn bản liên quan.

2: CSIRT không có văn bản chính thức về việc này, nhưng tự xây dựng tài liệu liên quan, chưa được phê duyệt chính thức.

3: CSIRT có văn bản tự xây dựng và do lãnh đạo đội phê duyệt.

4: CSIRT có văn bản chính thức do cấp trên phê duyệt về việc này và thường xuyên thực hiện đánh giá lại sự phù hợp.

VNO-4: Trách nhiệm

Trách nhiệm của CSIRT là những hoạt động mà CSIRT cần thực hiện để triển khai chức năng, nhiệm vụ của mình và đạt được các mục tiêu đảm bảo ứng

cứu kịp thời sự cố an toàn thông tin mạng cho các đối tượng mình phục vụ. Các CSIRT có quyết định thành lập chính thức thì trách nhiệm của CSIRT thường được nêu rõ trong quyết định này.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết về trách nhiệm của mình.

1: Các thành viên của CSIRT biết trách nhiệm của mình, nhưng chưa có văn bản nào nói về điều này.

2: CSIRT chưa có văn bản chính thức quy định về trách nhiệm của CSIRT, nên tự xây dựng dự thảo. Dự thảo này chưa được lãnh đạo phê duyệt.

3: CSIRT có văn bản chính thức quy định về trách nhiệm của mình do cấp trên phê duyệt.

4: CSIRT có văn bản chính thức do cấp trên phê duyệt. Trong quá trình hoạt động, các thành viên của CSIRT thường xuyên đánh giá định kỳ để hoàn thiện trách nhiệm của mình.

VNO-5: Danh mục các hoạt động nghiệp vụ

Hoạt động của CSIRT được triển khai theo các nhiệm vụ cụ thể, có phạm vi, mục tiêu rõ ràng. Các nhiệm vụ này cần được lập danh sách và mô tả nội dung đầy đủ để trở thành danh mục hoạt động nghiệp vụ của đơn vị. Trong số các hoạt động đó có phân tích mã độc, rà quét lỗ hổng, ứng cứu sự cố, giám sát, đào tạo, diễn tập, kiểm tra, đánh giá…

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa bao giờ đề cập đến điều này.

1: Các thành viên của CSIRT biết những hoạt động mà CSIRT cung cấp, nhưng chưa có văn bản nào thể hiện danh mục đó.

2: CSIRT đã tự xây dựng dự thảo liên quan danh mục các hoạt động nghiệp vụ

nhưng chưa phải văn bản chính thức.

3: CSIRT có bản mô tả danh mục các hoạt động, đã được lãnh đạo phê duyệt và đã được gửi tới các đối tác, khách hàng.

4: CSIRT đã có văn bản phê duyệt chính thức về danh mục các hoạt động nghiệp vụ, đã đưa vào triển khai và thực hiện đánh giá định kỳ để hoàn thiện.

VNO-6: Phân loại sự cố

Phân loại sự cố là việc làm bắt buộc của CSIRT. Các thông tin CSIRT thu thập và chia sẻ cần được phân loại theo kiểu loại thông tin, mức độ nghiêm trọng, mức độ ưu tiên để CSIRT có phương án xử lý hiệu quả khi có số lượng lớn các sự cố xảy ra đồng thời.

Điểm đánh giá:

0: Các thành viên của CSIRT không thực hiện phân loại sự cố và không có khái niệm về việc này.

1: Các thành viên của CSIRT hiểu rằng có nhiều loại sự cố khác nhau, cần phân loại, nhưng chưa thực hiện phân loại.

2: CSIRT không có văn bản chính thức về phân loại sự cố nên đã tự xây dựng tài liệu liên quan, chưa được lãnh đạo phê duyệt.

3: CSIRT có phân loại sự cố, đã được thể hiện bằng văn bản và đã được lãnh đạo phê duyệt.

4: CSIRT có văn bản phân loại sự cố đã được phê duyệt. Trong quá trình đánh giá định kỳ, CSIRT phân biệt các loại sự cố khác nhau và có cách thức xử lý phù hợp cho từng loại sự cố.

VNO-7: Quy chế hoạt động

CSIRT cần có quy chế hoạt động, hoặc điều lệ hoạt động, hoặc văn bản tương đương để bảo đảm việc vận hành đúng quy định, định hướng nhằm đạt được những mục tiêu đề ra.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: CSIRT có một quan điểm nhất quán về việc xây dựng quy chế hoạt động, nhưng chưa có văn bản nào thể hiện điều này.

2: CSIRT có dự thảo văn bản liên quan, nhưng chưa được phê duyệt.

3: CSIRT đã ban hành chính thức quy chế hoạt động.

4: CSIRT có quy chế hoạt động chính thức và đã triển khai, được đánh giá định kỳ để hoàn thiện.

VNO-8: Chính sách bảo mật

Bảo mật thông tin là chính sách quan trọng của CSIRT. Các CSIRT thực hiện phân cấp, phân quyền về bảo vệ bí mật thông tin, bảo vệ bí mật nội bộ phù hợp Luật Bảo vệ bí mật nhà nước số 29/2018/QH14 ngày ngày 15 tháng 11 năm 2018 và tuân thủ theo quy chế bảo vệ bí mật của đơn vị.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa quan tâm đến chính sách bảo mật thông tin và chưa bao giờ đề cập đến điều này.

1: Các thành viên của CSIRT biết về việc cần thực hiện bảo mật thông tin, nhưng chưa có văn bản nào thể hiện điều này.

2: CSIRT có dự thảo văn bản liên quan nhưng chưa được phê duyệt.

3: CSIRT đã có văn bản chính thức quy định về việc bảo mật thông tin.

4: CSIRT đã có văn bản chính thức quy định về việc bảo mật thông tin, đã triển khai và được đánh giá định kỳ để hoàn thiện.

3.2. Nhóm chỉ số đánh giá về con người (Human)

VNH-1: Quy tắc ứng xử

Tham gia đội ngũ CSIRT, các thành viên cần có những kiến thức, kỹ năng, thái độ làm việc tương ứng. Tài liệu hướng dẫn hoặc bộ quy tắc về cách ứng xử chuyên nghiệp, thực hiện đạo đức nghề nghiệp, tuân thủ bảo mật thông tin là yêu cầu đầu tiên mà CSIRT nên hoàn thành.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết các quy tắc ứng xử mình cần có là gì.

1: Các thành viên của CSIRT hiểu rõ quy tắc ứng xử cần có đối với vị trí của mình, nhưng chưa có văn bản nào thể hiện điều này.

2: CSIRT có dự thảo về quy tắc ứng xử của nhân sự CSIRT, nhưng chưa được phê duyệt.

3: CSIRT đã có văn bản chính thức do lãnh đạo phê duyệt.

4: CSIRT đã có văn bản chính thức được phê duyệt, đã triển khai, và được đánh giá định kỳ để hoàn thiện.

VNH-2: Phương án dự phòng nhân sự

Ứng cứu sự cố luôn yêu cầu có kế hoạch dự phòng về nhân sự ở tất cả các vị trí của CSIRT, nhằm giảm thiểu các rủi ro khi nhân sự nghỉ việc, bỏ việc, luân chuyển vị trí việc làm hoặc vì các lý do bất khả kháng khác. Kế hoạch dự phòng này đảm bảo tính liên tục hoạt động của CSIRT. Các nhân sự dự phòng cần đảm bảo có kỹ năng đầy đủ để đảm đương được nhiệm vụ được giao.

Điểm đánh giá:

0: CSIRT không có nhân sự dự phòng và việc này nằm ngoài phạm vi quyết định của CSIRT.

1: CSIRT có đủ người dự phòng trong công việc, nhưng kế hoạch dự phòng chưa được viết ra thành văn bản.

2: CSIRT đã có kế hoạch dự phòng nhân sự được viết ra thành văn bản, nhưng

chưa được lãnh đạo chính thức phê duyệt.

3: CSIRT có văn bản chính thức về số lượng nhân viên và kế hoạch dự phòng nhân sự, đã được lãnh đạo phê duyệt.

4: CSIRT có kế hoạch dự phòng nhân sự đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra thực tế hiệu quả của kế hoạch và thực hiện điều chỉnh (nếu cần).

VNH-3: Yêu cầu về kỹ năng

Mỗi vị trí việc làm tại CSIRT cần có bản mô tả rõ ràng về trình độ, kỹ năng cần có. Bản mô tả này phục vụ cho công tác tuyển dụng, bố trí công việc và đào tạo tại CSIRT.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT biết mình cần phải có những kỹ năng gì, nhưng chưa có văn bản nào mô tả hay đưa ra yêu cầu về những kỹ năng đó.

2: CSIRT không có văn bản mô tả các kỹ năng cần phải có cho các vị trí công việc. Do vậy, các thành viên của CSIRT đã tự viết tài liệu để sử dụng riêng, lãnh đạo chưa phê duyệt.

3: CSIRT có tài liệu mô tả các kỹ năng cần thiết cho từng vị trí việc làm tại CSIRT. Văn bản này đã được phê duyệt.

4: CSIRT có bản mô tả kỹ năng đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem bộ kỹ năng này có đủ để triển khai hoạt động, giải quyết công việc, thực hiện xử lý các sự cố an toàn thông tin hay không.

VNH-4: Phát triển đội ngũ

CSIRT cần phát triển đội ngũ nhân sự, đặc biệt về chuyên môn, nghiệp vụ. Hàng năm CSIRT có kế hoạch đào tạo nhân sự phù hợp thực tế, đó là các hoạt

động đào tạo nội bộ, đào tạo bên ngoài, các hoạt động nhóm, các hoạt động tập thể (team building) và lộ trình phát triển cho từng cá nhân.

Điểm đánh giá:

0: CSIRT không thực hiện các hoạt động phát triển đội ngũ.

1: CSIRT có ý tưởng về phát triển đội ngũ và các thành viên của CSIRT đã tự đào tạo nhau, nhưng chưa có văn bản nào thể hiện việc làm này.

2: CSIRT không có chương trình phát triển đội ngũ chính thức, do đó các thành viên của CSIRT đã tự viết tài liệu sử dụng riêng. Tài liệu này chưa được lãnh đạo phê duyệt.

3: CSIRT có một chương trình phát triển đội ngũ đã được lãnh đạo phê duyệt.

4: CSIRT có một chương trình phát triển đội ngũ được lãnh đạo phê duyệt. Trong quá trình đánh giá định kỳ, các thành viên của CSIRT sẽ kiểm tra xem chương trình này đã đáp ứng nhu cầu của tổ chức hay chưa.

VNH-5: Đào tạo kỹ thuật

CSIRT là tổ chức chuyên sâu về kỹ thuật, do vậy ngoài việc tự đào tạo kỹ thuật trong nội bộ, đội ngũ kỹ thuật của CSIRT cần được tham gia các khóa đào tạo bên ngoài, thi các chứng chỉ quốc gia và quốc tế để cập nhật kiến thức, công nghệ mới. Các thành viên CSIRT cần tham gia đầy đủ các hoạt động diễn tập quốc tế và diễn tập trong nước (bao gồm các diễn tập thực chiến do Bộ Thông tin và Truyền thông (Cục An toàn thông tin) tổ chức. CSIRT có thể tự triển khai hoặc lựa chọn tổ chức, doanh nghiệp có đủ năng lực để triển khai diễn tập thực chiến nhằm thực hành và cải thiện năng lực phòng thủ của đội ứng cứu sự cố.

Điểm đánh giá:

0: CSIRT không thực hiện loại hình đào tạo này.

1: Các thành viên của CSIRT cử người tham gia các khóa đào tạo như vậy khi

cần thiết, nhưng CSIRT không có văn bản nào quy định về việc này.

2: CSIRT chưa có hướng dẫn, quy định chính thức về việc đào tạo này. Tuy nhiên, các thành viên CSIRT đã tự xây dựng một bộ tài liệu liên quan, lãnh đạo chưa phê duyệt.

3: CSIRT có kế hoạch cử nhân viên đi đào tạo kỹ thuật bên ngoài và đã được phê duyệt.

4: CSIRT có kế hoạch, chương trình đào tạo kỹ thuật bên ngoài đã được phê duyệt. Chương trình này cho phép các nhân viên của CSIRT được gửi đi đào tạo tại các tổ chức khác. Trong quá trình đánh giá định kỳ, chương trình đào tạo kỹ thuật này được xem xét là đủ để đáp ứng nhu cầu đào tạo của CSIRT hay chưa.

VNH-6: Đào tạo kỹ năng mềm

Các thành viên CSIRT cần được đào tạo bài bản, chuyên nghiệp để biết cách hành xử, tương tác với xung quanh đúng đắn khi có sự cố xảy ra, như cung cấp thông tin cho báo chí; viết email, gọi điện thoại thực hiện báo cáo xử lý sự cố; tư vấn trực tiếp cho các khách hàng, đối tác về hoạt động ứng cứu sự cố; trình bày báo cáo trước tập thể.

Điểm đánh giá:

0: CSIRT không thực hiện loại hình đào tạo này.

1: CSIRT có cử người tham gia các khóa đào tạo như vậy khi cần, nhưng CSIRT chưa có văn bảo nào nói về việc này.

2: CSIRT chưa có chương trình đào tạo kỹ năng mềm chính thức, nhưng đã có đề xuất cụ thể về việc này.

3: CSIRT có chủ trương, chương trình đào tạo về kỹ năng mềm đã được phê duyệt. Đây là căn cứ để CSIRT cử nhân viên của mình tham gia các khóa đào tạo như vậy.

4: CSIRT có chủ trương, kinh phí, chương trình đào tạo về kỹ năng mềm đã

được phê duyệt. Trong quá trình đánh giá định kỳ, CSIRT sẽ kiểm tra xem chương trình đào tạo này đã đủ để đáp ứng nhu cầu đào tạo của đơn vị hay chưa và tiến hành hoàn thiện.

VNH-7: Kết nối - hợp tác

Các thành viên của CSIRT tích cực tham gia vào các sự kiện, mở rộng quan hệ kết nối. Việc xây dựng các kênh liên lạc giữa các chuyên gia sẽ giúp cho các tổ chức gắn kết và thúc đẩy công việc được xử lý hiệu quả, nhanh chóng.

Điểm đánh giá:

0: CSIRT không có thời gian hoặc kinh phí cho loại hoạt động này.

1: Các thành viên của CSIRT có tham gia các sự kiện như vậy, nhưng không theo kế hoạch hay văn bản quy định, hướng dẫn nào.

2: CSIRT không có chính sách, quy định về việc kết nối mạng lưới chuyên gia bên ngoài. Các thành viên của CSIRT đã đưa ra đề xuất về việc này.

3: CSIRT có văn bản chính thức (chính sách, định hướng, quy định...) về việc kết nối mạng lưới chuyên gia.

4: CSIRT có văn bản chính thức về việc kết nối các chuyên gia, được lãnh đạo chấp thuận. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem CSIRT có tích cực theo đuổi mạng lưới chuyên gia này hay không và lợi ích là gì.

3.3. Nhóm chỉ số đánh giá về công cụ (Tool)

VNT-1: Danh sách tài nguyên công nghệ thông tin

CSIRT phải có danh sách tài nguyên công nghệ thông tin mà mình chịu trách nhiệm bảo vệ. Danh sách này được thống kê cập nhật và quản lý tập trung bằng công cụ để tiện theo dõi và cập nhật.

Điểm đánh giá:

0: CSIRT không có danh sách này và các thành viên của CSIRT hoàn toàn

không có ý tưởng gì về danh sách này.

1: CSIRT không có danh sách này nhưng các thành viên hiểu rằng việc nắm danh sách các tài nguyên CNTT là rất quan trọng để triển khai hoạt động ứng cứu sự cố an toàn thông tin mạng.

2: CSIRT có danh sách tài nguyên CNTT tự xây dựng, nhưng danh sách chưa được lãnh đạo phê duyệt.

3: CSIRT có danh sách tài nguyên CNTT đã được phê duyệt.

4: CSIRT có danh sách tài nguyên CNTT đã được phê duyệt, được theo dõi và quản lý bằng công cụ. Trong quá trình đánh giá định kỳ, các thành viên của CSIRT sẽ kiểm tra xem danh sách này có hữu ích và đủ chính xác để hoàn thành các nhiệm vụ đề ra hay không.

VNT-2: Danh sách nguồn thông tin

CSIRT phải có danh sách các nguồn thông tin về nguy cơ các tấn công mạng, khai thác lỗ hổng, tấn công mã độc... Các nguồn thông tin này được tổng hợp và theo dõi dựa trên các công cụ, hệ thống kỹ thuật cụ thể.

Điểm đánh giá:

0: CSIRT không có danh sách nguồn thông tin. CSIRT nhận được thông tin sự cố thì xử lý và không kiểm tra nguồn.

1: CSIRT không có danh sách này, nhưng các thành viên của CSIRT hiểu tầm quan trọng của nguồn thông tin và có kiểm tra nguồn.

2: CSIRT có danh sách các nguồn thông tin tự xây dựng, nhưng chưa chính thức, do chưa được lãnh đạo phê duyệt.

3: CSIRT có một danh sách chính thức các nguồn thông tin đã được phê duyệt.

4: CSIRT có danh sách chính thức các nguồn thông tin. Trong quá trình đánh giá định kỳ, các thành viên của CSIRT sẽ kiểm tra xem danh sách này có hữu ích

và đủ để hoàn thành nhiệm vụ, đạt được các mục tiêu không.

VNT-3: Kênh thông tin liên lạc không gián đoạn

Thông tin liên lạc có vai trò đặc biệt quan trọng trong ứng cứu sự cố an toàn thông tin mạng. Các kênh trao đổi thông tin qua điện thoại, email cần đảm bảo thông suốt, luôn có dự phòng thay thế để không bị gián đoạn hoạt động. CSIRT cần có đầy đủ các công cụ để đảm bảo cho hoạt động này.

Điểm đánh giá:

0: Tổ chức chưa có kênh liên lạc dành riêng cho hoạt động đảm bảo an toàn thông tin mạng.

1: Tổ chức đã có kênh riêng dành cho các hoạt động đảm bảo an toàn thông tin mạng, tuy nhiên các kênh này hoạt động chưa ổn định và chưa có đa dạng hình thức liên lạc.

2: Tổ chức có đa dạng kênh liên lạc chuyên trách dành riêng cho CSIRT, tuy nhiên chưa có phương án dự phòng khi các kênh này gặp sự cố.

3: CSIRT có hệ thống các kênh liên lạc riêng, hoạt động ổn định và luôn có phương án dự phòng, tuy nhiên, chưa có văn bản nào thể hiện việc bố trí các kênh liên lạc cùng các phương án dự phòng này.

4: CSIRT có hệ thống các kênh liên lạc riêng, hoạt động ổn định và luôn có phương án dự phòng. Việc bố trí các kênh liên lạc cùng các phương án dự phòng đã được ban hành thành văn bản chính thức.

VNT-4: Hệ thống theo dõi sự cố

CSIRT cần có hệ thống theo dõi sự cố hoặc sử dụng nền tảng IRLab (irlab.vn) nhằm đảm bảo các sự cố được cập nhật, theo dõi và xử lý thường xuyên, có hệ thống quản lý log tập trung được triển khai để thu thập và lưu trữ các sự kiện được sinh ra từ các hệ thống, thiết bị. Thông qua các hệ thống này, CSIRT nắm bắt được quá trình xử lý của đội ngũ theo luồng công việc.

Điểm đánh giá:

0: CSIRT không có công cụ đăng ký, quản lý các sự cố.

1: CSIRT thực hiện đăng ký, theo dõi các sự cố, nhưng chưa ghi lại việc này.

2: CSIRT có hệ thống theo dõi sự cố, nhưng chưa được lãnh đạo phê duyệt.

3: CSIRT có một hệ thống theo dõi sự cố và đã được phê duyệt.

4: CSIRT có một hệ thống theo dõi sự cố đã được phê duyệt. Trong quá trình đánh giá định kỳ, hệ thống theo dõi này sẽ được kiểm tra xem có đáp ứng các yêu cầu của CSIRT hay không.

VNT-5: Đảm bảo kết nối internet ổn định

Việc đảm bảo tính ổn định của kết nối internet rất quan trọng trong ứng cứu sự cố. Vì vậy CSIRT phải có phương án đảm bảo khả năng truy cập internet liên tục, thông suốt, không gián đoạn.

Điểm đánh giá:

0: CSIRT không có kết nối internet.

1: CSIRT có kết nối internet, nhưng đường truyền không ổn định.

2: Kết nối internet của CSIRT ổn định, có tài liệu hướng dẫn và quản lý kết nối nhưng chưa ban hành chính thức.

3: Kết nối internet của CSIRT ổn định và CSIRT có tài liệu được phê duyệt về việc này.

4: Đường truyền truy cập internet của CSIRT ổn định cho các hoạt động của CSIRT và CSIRT có tài liệu quy định việc này. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem khả năng truy cập internet như vậy có đủ hay không.

VNT-6: Bộ công cụ phòng ngừa sự cố

CSIRT cần có các công cụ phòng ngừa sự cố, ngăn chặn các cuộc tấn công liên quan đến mã độc, các biện pháp kỹ thuật, công nghệ, sử dụng các công

cụ có khả năng phục hồi nhanh, đưa hệ thống về trạng thái hoạt động ban đầu khi sự cố xảy ra.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về bộ công cụ này.

1: CSIRT có những công cụ như vậy, nhưng chưa liệt kê hoặc ghi lại chúng.

2: CSIRT có những công cụ như vậy, đã lập danh sách, nhưng chưa được lãnh đạo phê duyệt.

3: CSIRT có các công cụ như vậy, đã có danh sách được phê duyệt.

4: CSIRT có các công cụ như vậy, đã lập danh sách và đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem những công cụ này có đủ đáp ứng các yêu cầu của CSIRT hay không.

VNT-7: Bộ công cụ phát hiện sự cố

CSIRT cần có các công cụ phát hiện sự cố, các kỹ thuật, công nghệ cho phép đội CSIRT chủ động thực hiện các hoạt động truy tìm các mối đe dọa an toàn thông tin đang ẩn náu bên trong hệ thống.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về bộ công cụ này.

1: CSIRT có những công cụ như vậy, nhưng chưa liệt kê hoặc ghi lại chúng.

2: CSIRT có những công cụ như vậy, đã có danh sách nhưng chưa được lãnh đạo cấp trên phê duyệt.

3: CSIRT có các công cụ như vậy, đã lập danh sách và đã được phê duyệt.

4: CSIRT có các công cụ như vậy, đã lập danh sách, đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem những công cụ này có đủ đáp ứng các yêu cầu của CSIRT hay không.

VNT-8: Hệ thống xử lý sự cố

CSIRT cần có hệ thống xử lý sự cố gồm các công cụ xử lý các hoạt động tấn công, xâm nhập trên mạng và trên các hệ thống máy tính nhằm theo dõi, phát hiện và ngăn chặn các sự cố kịp thời.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về công cụ này.

1: CSIRT có những công cụ như vậy, nhưng chưa liệt kê hoặc ghi lại chúng.

2: CSIRT có những công cụ như vậy, đã lập danh sách, nhưng chưa được lãnh đạo phê duyệt.

3: CSIRT có các công cụ như vậy, đã lập danh sách và đã được phê duyệt.

4: CSIRT có các công cụ như vậy, đã lập danh sách và đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem những công cụ này có đủ đáp ứng các yêu cầu của CSIRT hay không.

3.4. Nhóm chỉ số đánh giá về quy trình (Processes)

VNP-1: Quy trình báo cáo sự cố lên cấp quản lý cao hơn

CSIRT cần có quy trình báo cáo sự cố đến cấp quản lý cao hơn. Quy trình này được kích hoạt tùy theo mức độ nghiêm trọng của từng loại sự cố cụ thể. Quy trình báo cáo này cần được xây dựng thành văn bản, phù hợp với các quy định tại Điều 11, Quyết định số 05/2017/QĐ-TTg.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về việc báo cáo này.

1: CSIRT có thực hiện báo cáo lên các cấp cao hơn, nhưng việc làm này chưa được lập thành văn bản.

2: CSIRT có quy trình báo cáo bằng văn bản tự xây dựng, nhưng chưa được lãnh đạo phê duyệt.

3: CSIRT có quy trình báo cáo chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có quy trình báo cáo chính thức bằng văn bản đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này đã được sử dụng một cách thích hợp chưa và hoạt động như thế nào.

VNP-2: Quy trình công khai thông tin

Thông tin liên quan các sự cố và hoạt động ứng cứu khi xuất hiện trên các phương tiện truyền thông đại chúng hay trên internet phải được lựa chọn, được sự phê duyệt của lãnh đạo, tuân thủ theo quy trình nhằm đảm bảo tính chính xác, kịp thời, phù hợp và bí mật của thông tin.

Điểm đánh giá:

0: CSIRT chưa bao giờ công khai thông tin hoạt động của mình trên báo chí hay internet.

1: CSIRT có thực hiện cung cấp thông tin cho báo chí và công khai trên internet, tuy nhiên chưa có văn bản nào hướng dẫn hay ghi lại cách làm.

2: CSIRT đã xây dựng văn bản liên quan (hướng dẫn, quy định) việc cung cấp thông tin cho báo chí, công khai trên internet nhưng chưa được phê duyệt.

3: CSIRT đã ban hành quy trình cung cấp thông tin cho báo chí, công khai trên internet.

4: CSIRT có một quy trình cung cấp thông tin cho báo chí, công khai trên internet đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này đã được sử dụng một cách thích hợp chưa và nó hoạt động như thế nào.

VNP-3: Quy trình cung cấp thông tin cho cơ quan pháp lý

Tấn công mạng khi không được phép là vi phạm pháp luật. CSIRT cần có quy trình cung cấp thông tin cho các cơ quan pháp lý khi có tấn công mạng xảy ra hoặc nghi ngờ bị tấn công mạng để nhanh chóng hỗ trợ các cơ quan chức năng xử lý các vụ việc vi phạm pháp luật này.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: CSIRT có thực hiện cung cấp thông tin cho cơ quan pháp lý, tuy nhiên chưa có văn bản nào ghi lại điều này.

2: CSIRT có dự thảo văn bản về việc cung cấp thông tin cho cơ quan pháp lý, nhưng chưa được phê duyệt.

3: CSIRT có một quy trình cung cấp thông tin cho cơ quan pháp lý đã được lập thành văn bản và đã được phê duyệt.

4: CSIRT có quy trình cung cấp thông tin cho cơ quan pháp lý chính thức. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này đã được sử dụng một cách thích hợp chưa và hoạt động như thế nào.

VNP-4: Quy trình phòng ngừa sự cố

Quy trình phòng ngừa sự cố là một trong những quy trình cần được xây dựng đầu tiên khi vận hành CSIRT. Các hoạt động nâng cao nhận thức, công bố các thông tin về lỗ hổng bảo mật đã phát hiện được, và công bố các sự cố xảy ra trong quá khứ, ban hành phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin và cập nhật kịp thời khi có thay đổi là một phần của nội dung quy trình này.

Điểm đánh giá:

0: Các thành viên CSIRT đã có hoạt động phòng ngừa, ngăn chặn sự cố nhưng bị động, chưa có ý thức về điều này.

1: Các thành viên của CSIRT biết cách triển khai, đã chủ động thực hiện hoạt động phòng ngừa, ngăn chặn sự cố, nhưng chưa xây dựng thành văn bản.

2: CSIRT đã dự thảo quy trình phòng ngừa sự cố nhưng chưa được lãnh đạo phê duyệt.

3: CSIRT đã có quy trình phòng ngừa sự cố chính thức.

4: CSIRT có quy trình phòng ngừa sự cố chính thức. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này hoạt động như dự kiến không.

VNP-5: Quy trình phát hiện sự cố

Quy trình phát hiện sự cố được triển khai thường xuyên tại CSIRT. Các công cụ như hệ thống email, điện thoại, đường truyền internet giúp CSIRT thu thập thông tin cũng là một phần của quy trình này.

Điểm đánh giá:

0: Các thành viên của CSIRT biết cách thực hiện nhiệm vụ này, nhưng chưa ghi lại thành văn bản.

1: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

2: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-6: Quy trình xử lý sự cố

Quy trình xử lý sự cố làm rõ các hoạt động cần thực hiện để xử lý các sự cố khi được phát hiện và mô tả việc sử dụng các công cụ xử lý sự cố.

CSIRT đạt mức trưởng thành cao hơn khi có quy trình xử lý các sự cố cụ thể. Bao gồm các loại tấn công điển hình như tấn công sử dụng mã độc, tấn công DDOS, tấn công lừa đảo (phishing), tấn công khai thác lỗ hổng ứng dụng web, tấn công sử dụng mã độc đòi tiền chuộc (ransomware).

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT biết cách thực hiện việc này, nhưng chưa ghi lại

thành văn bản.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có quy trình chính thức bằng văn bản. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến không.

VNP-7: Quy trình đánh giá hoàn thiện tổ chức

Để liên tục hoàn thiện tổ chức, CSIRT cần có quy trình mô tả cách thức xây dựng và phát triển tổ chức, các khía cạnh về con người, hoạt động, quy trình để thường xuyên tự đánh giá, kiểm tra, phản hồi và khắc phục liên hoàn. Nếu những yếu tố cũ không còn phù hợp với các tiêu chuẩn mới thì cần được thay đổi, cập nhật.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa có ý thức về điều này.

1: CSIRT đã có đánh giá tổng thể về chính đội ngũ của mình để điều chỉnh, nhưng chưa có văn bản nào thể hiện điều đó.

2: CSIRT đã dự thảo quy trình, nhưng chưa chính thức.

3: CSIRT đã ban hành chính thức quy trình đánh giá hoàn thiện tổ chức.

4: CSIRT có quy trình chính thức bằng văn bản được phê duyệt bởi cấp quản lý cao hơn.

VNP-8: Quy trình tiếp cận khẩn cấp

Trong ứng cứu sự cố, đặc biệt ứng cứu khẩn cấp, CSIRT và các bên liên quan cần có các quy trình thông tin liên lạc phù hợp. Tùy theo từng mức độ nghiêm trọng của sự cố, việc thông báo được thực hiện theo các kênh kết nối đã được xây dựng trước: kết nối với chuyên viên hay trực tiếp với lãnh đạo của

CSIRT; ai, đội, nhóm hay đơn vị nào có thể liên lạc với đại diện CSIRT; cách liên lạc, truyền đạt thông tin thế nào, tối mật hay công khai để đảm bảo thời gian xử lý công việc nhanh và hiệu quả nhất.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa có ý tưởng gì về quy trình này.

1: Trong trường hợp khẩn cấp, các bên liên quan biết cách liên hệ với các thành viên của CSIRT, nhưng CSIRT chưa có văn bản nào đề cập vấn đề này.

2: CSIRT có dự thảo quy trình, nhưng chưa được lãnh đạo phê duyệt.

3: CSIRT có quy trình chính thức bằng văn bản đã gửi cho các bên liên quan.

4: CSIRT có quy trình chính thức bằng văn bản gửi cho các bên liên quan. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-9: Quy trình xử lý thông tin mật

CSIRT cần có các quy định về các bước xử lý thông tin quan trọng. Các báo cáo sự cố hoặc thông tin liên quan phải được xử lý như thông tin mật.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT biết cách bảo mật thông tin, nhưng chưa ghi lại thành văn bản.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có quy trình chính thức bằng văn bản đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-10: Quy trình quản lý nguồn tin

CSIRT cần có quy trình quản lý nguồn thông tin, thiết lập và lưu trữ tách biệt các dữ liệu liên quan đến hoạt động của người dùng, mạng và hệ thống. Quy trình triển khai chi tiết được phổ biến cho các cán bộ kỹ thuật đảm trách các nhiệm vụ này.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT biết cách làm điều này, nhưng không ghi lại thành văn bản.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-11: Quy trình tiếp cận đối tác, khách hàng

Quy trình tiếp cận các đối tác, khách hàng được xây dựng giúp CSIRT hoạt động chuyên nghiệp và tăng khả năng mở rộng quy mô phát triển. Quy trình này bao gồm tất cả các hình thức tiếp cận, các cách thức quản lý kết nối đối tác, khách hàng và các hình thức xuất hiện trên các trang web, bản tin, các hoạt động tư vấn cho đến các sự kiện như hội thảo, đào tạo, v.v.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên CSIRT biết cách thực hiện nhưng chưa ghi thành văn bản.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây

dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-12: Quy trình kết nối cơ quan quản lý nhà nước

CSIRT thực hiện kết nối, chia sẻ thông tin với các trung tâm giám sát an toàn thông tin mạng của quốc gia theo quy định của pháp luật; phối hợp chặt chẽ với cơ quan điều phối quốc gia về ứng cứu sự cố an toàn thông tin mạng, tham gia hoạt động ứng cứu khẩn cấp khi có yêu cầu từ cơ quan điều phối.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT biết cách thực hiện công việc, nhưng chưa ghi lại thành văn bản.

2: CSIRT chưa có quy trình chính thức nên các thành viên CSIRT đã tự xây dựng tài liệu liên quan, chưa được lãnh đạo phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có một quy trình chính thức bằng văn bản đã được quản lý cấp trên phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-13: Quy trình thống kê sự cố

CSIRT cần có quy trình thống kê và phân loại sự cố, đánh giá đúng mức độ của từng sự kiện, từng loại sự cố. Các sự cố cần được thống kê và chia sẻ trên Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia (irlab.vn). Các quy trình phân loại sự cố này có ảnh hưởng quan trọng đến việc ra các quyết định tiếp theo của CSIRT trong ứng cứu sự cố, đặc biệt đến việc áp dụng các

quy trình ứng cứu sự cố thông thường và ứng cứu sự cố an toàn thông tin mạng nghiêm trọng tại điều 13, 14 của Quyết định 05/2017/QĐ-TTg.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa thảo luận về việc cần có một quy trình thống kê sự cố.

1: Các thành viên của CSIRT có thực hiện thống kê và phân loại sự cố, nhưng việc này chưa được ghi lại thành văn bản.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có quy trình chính thức bằng văn bản đã được phê duyệt. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-14: Quy trình họp

CSIRT cần có quy trình, quy định cụ thể về họp giao ban, họp thường kỳ, họp đột xuất và các bước cần thực hiện khi tổ chức các cuộc họp như vậy. Mỗi cuộc họp cần có chủ trì, thư ký chương trình làm việc và biên bản họp.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT gặp nhau thường xuyên, tổ chức họp thường xuyên, nhưng không có văn bản nào ghi lại điều này.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có quy trình chính thức bằng văn bản đã được phê duyệt. Trong quá

trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

VNP-15: Quy trình phối hợp trong Mạng lưới

CSIRT thuộc thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia cần có quy trình phối hợp với các CSIRT của các thành viên khác trong Mạng lưới và thực hiện hoạt động ứng cứu sự cố theo các quy định hiện hành của Chính phủ và hướng dẫn của các cơ quan quản lý nhà nước.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và chưa thảo luận về điều này.

1: Các thành viên của CSIRT biết cách thực hiện, nhưng chưa ghi lại thành văn bản về hoạt động này.

2: CSIRT không có quy trình chính thức, nhưng có tài liệu liên quan tự xây dựng, chưa được lãnh đạo phê duyệt.

3: CSIRT có một quy trình chính thức bằng văn bản đã được phê duyệt.

4: CSIRT có quy trình chính thức bằng văn bản. Trong quá trình đánh giá định kỳ, tổ chức sẽ kiểm tra xem quy trình này có hoạt động như dự kiến hay không.

3.5. Nhóm chỉ số đánh giá về hoạt động thường xuyên (Activities)

VNA-1: Kế hoạch hoạt động hàng năm

Kế hoạch hoạt động thường xuyên của CSIRT cần được xây dựng hàng năm từ cuối năm trước và ban hành vào đầu năm sau. Một tổ chức hoạt động hiệu quả cần có mục tiêu và chương trình triển khai hoạt động cụ thể. Đối với CSIRT, các kế hoạch hoạt động nhằm triển khai các hoạt động ứng cứu sự cố là nội dung cần được thực hiện đầu tiên.

Điểm đánh giá:

0: CSIRT chưa có kế hoạch hoạt động.

1: CSIRT đã xây dựng kế hoạch hoạt động nhưng chưa ban hành chính thức.

2: CSIRT đã có kế hoạch hoạt động chính thức và đã được triển khai.

3: CSIRT đã có kế hoạch hoạt động được ban hành chính thức, được cấp kinh phí triển khai theo kế hoạch và đã hoàn thành kế hoạch đề ra.

4: CSIRT đã có kế hoạch hoạt động được ban hành chính thức, được cấp kinh phí triển khai theo kế hoạch, và kế hoạch đã được hoàn thành để có các kế hoạch triển khai tiếp theo giúp mở rộng hoạt động và phát triển tổ chức.

VNA-2: Tham gia thường xuyên nền tảng IRLab

Sử dụng thường xuyên Nền tảng điều phối xử lý sự cố an toàn thông tin mạng quốc gia - IRLab (irlab.vn) để báo cáo sự cố, tiếp nhận cảnh báo từ cơ quan điều phối quốc gia. Việc theo dõi, cập nhật các lỗ hổng bảo mật, các nguy cơ tấn công mạng, chiến dịch mã độc được Cục An toàn thông tin chia sẻ tới từng đơn vị tham gia.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết đến việc tham gia nền tảng này.

1: CSIRT đã tham gia, nhưng các thành viên trong đội không nắm được các hoạt động nghiệp vụ được thực hiện trên nền tảng.

2: Việc sử dụng Nền tảng để tiếp nhận cảnh báo, theo dõi, xử lý, gửi báo cáo sự cố được phổ biến đến tất cả các thành viên trong CSIRT.

3: CSIRT đã tham gia nền tảng, thực hiện tiếp nhận và phản hồi, xử lý kịp thời các cảnh báo, sự cố liên quan đến tổ chức mình từ cơ quan điều phối quốc gia.

4: CSIRT đã tham gia thường xuyên, tiếp nhận, phản hồi và xử lý kịp thời các cảnh báo, sự cố từ cơ quan điều phối quốc gia. CSIRT tích cực chia sẻ tri thức về ứng cứu sự cố cho các thành viên khác trong toàn mạng lưới, được VNCERT/CC đánh giá cao và đã tuyên truyền, phổ biến, hướng dẫn đến các đơn vị khác cùng tham gia.

VNA-3: Rà quét lỗ hổng

Để giảm thiểu tối đa các sự cố gây ra bởi lỗ hổng bảo mật, CSIRT cần chủ động thực hiện rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/06 tháng bằng cách sử dụng công cụ sẵn có.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa thực hiện rà quét lỗ hổng trên các hệ thống thông tin được giao trách nhiệm bảo vệ.

1: Các thành viên của CSIRT đã tìm cách rà quét lỗ hổng trên các hệ thống thông tin được giao trách nhiệm bảo vệ nhưng thiếu công cụ thực hiện.

2: CSIRT đã sử dụng công cụ để thực hiện rà quét lỗ hổng trên các hệ thống thông tin được giao trách nhiệm bảo vệ nhưng không thường xuyên.

3: CSIRT đã thường xuyên sử dụng công cụ để thực hiện rà quét lỗ hổng trên các hệ thống thông tin được giao trách nhiệm bảo vệ tối thiểu 01 lần/06 tháng, nhưng không xử lý triệt để các lỗ hổng được phát hiện.

4: CSIRT đã thực hiện rà quét lỗ hổng trên các hệ thống thông tin được giao trách nhiệm bảo vệ tối thiểu 01 lần/06 tháng và đã phát hiện, xử lý kịp thời các lỗ hổng tồn tại trên hệ thống thông qua việc cấu hình lại máy chủ, thiết bị tường lửa và cập nhật mã nguồn.

VNA-4: Săn lùng mối nguy

CSIRT cần chủ động thực hiện săn lùng mối nguy hại trên các hệ thống thông tin trong phạm vi quản lý tối thiểu 01 lần/06 tháng. Trường hợp phát hiện điểm yếu, lỗ hổng bảo mật cho phép xâm nhập và kiểm soát hệ thống thì thực hiện đồng thời khắc phục điểm yếu, lỗ hổng và săn lùng mối nguy hại.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa thực hiện săn lùng mối nguy trên các hệ

thống thông tin được giao trách nhiệm bảo vệ.

1: Các thành viên của CSIRT đã tìm cách săn lùng mối nguy trên các hệ thống thông tin được giao trách nhiệm bảo vệ nhưng thiếu công cụ thực hiện.

2: CSIRT đã sử dụng công cụ để thực hiện săn lùng mối nguy trên các hệ thống thông tin được giao trách nhiệm bảo vệ nhưng không thường xuyên.

3: CSIRT đã thường xuyên săn lùng mối nguy tối thiểu 01 lần/ 06 tháng trên các hệ thống thông tin được giao trách nhiệm bảo vệ nhưng thiếu đội ngũ chuyên gia để phân tích chuyên sâu.

4: CSIRT đã thực hiện săn lùng mối nguy hại trên các hệ thống thông tin được giao trách nhiệm bảo vệ tối thiểu 01 lần/06 tháng và đã phát hiện, xử lý kịp thời các mối nguy cho hệ thống; đồng thời yêu cầu chuyên gia, các cơ quan chuyên môn hỗ trợ thực hiện phân tích chuyên sâu và cải thiện hệ thống phòng thủ để ngăn chặn các mối đe dọa tương tự trong tương lai.

VNA-5: Diễn tập thực chiến

Đối với hệ thống thông tin cấp độ 3 trở lên, CSIRT cần đề xuất phương án, kế hoạch tổ chức diễn tập thực chiến tối thiểu 01 lần/năm; CSIRT cần tham gia trực tiếp vào hoạt động thực chiến của cơ quan mình, của cụm mạng lưới và các hoạt động diễn tập thực chiến quốc gia nhằm rèn luyện khả năng phát hiện, ngăn chặn tấn công trong thực tế.

Điểm đánh giá:

0: Các thành viên của CSIRT chưa biết và hiểu về diễn tập thực chiến.

1: Các thành viên của CSIRT đã hiểu biết về diễn tập thực chiến nhưng chưa tham gia.

2: CSIRT đã tham gia các hoạt động diễn tập thực chiến quy mô nhỏ.

3: CSIRT đã tự xây dựng kế hoạch tổ chức diễn tập thực chiến với sự tham gia của tất cả các thành viên CSIRT mà đơn vị quản lý.

4: CSIRT tham gia đầy đủ các hoạt động diễn tập thực chiến, được VNCERT/CC đánh giá cao về việc tổ chức và chất lượng hoạt động.

VNA-6: Chia sẻ thông tin

CSIRT thường xuyên chia sẻ, cập nhật kịp thời các thông tin, tri thức liên quan đến sự cố, lỗ hổng bảo mật, mã độc, các phương thức tấn công mạng mà tổ chức mình gặp phải tới cơ quan điều phối quốc gia về ứng cứu sự cố, các thành viên trong Mạng lưới thông qua nền tảng IRLab và các cơ quan quản lý nhà nước theo quy định của pháp luật.

Điểm đánh giá:

0: CSIRT không chia sẻ thông tin về sự cố, không cập nhật thông tin liên quan sự cố với bất kỳ đơn vị nào.

1: CSIRT tuân thủ việc báo cáo sự cố mà tổ chức mình gặp phải cho Trung tâm VNCERT/CC, nhưng không chia sẻ thông tin sự cố trong Mạng lưới.

2: CSIRT tuân thủ việc báo cáo sự cố mà tổ chức mình gặp phải cho Trung tâm VNCERT/CC; thực hiện chia sẻ thông tin liên quan đến sự cố tới toàn bộ thành viên Mạng lưới ở mức hạn chế, nhưng không theo cơ chế chia sẻ thông tin liên quan đến sự cố được báo cáo trên nền tảng IRLab.

3: CSIRT tuân thủ việc báo cáo sự cố mà tổ chức mình gặp phải cho Trung tâm VNCERT/CC; thực hiện chia sẻ thông tin liên quan đến sự cố thông qua nền tảng IRLab theo đúng cơ chế chia sẻ thông tin liên quan đến sự cố được báo cáo trên nền tảng IRLab.

4: CSIRT tuân thủ việc báo cáo sự cố mà tổ chức mình gặp phải cho Trung tâm VNCERT/CC; thực hiện chia sẻ thông tin liên quan đến sự cố thông qua nền tảng IRLab theo đúng cơ chế chia sẻ thông tin liên quan đến sự cố được báo cáo trên nền tảng IRLab; thường xuyên chia sẻ, cập nhật các thông tin, tri thức liên quan đến hoạt động tấn công mạng cho các thành viên trong Mạng lưới.

Phụ lục I
MÔ HÌNH ĐÁNH GIÁ MỨC ĐỘ TRƯỞNG THÀNH CỦA CSIRT TẠI VIỆT NAM GIAI ĐOẠN 1

Giai đoạn 1 thực hiện đánh giá mức độ trưởng thành của CSIRT dựa trên ***22 chỉ số*** sau:

STT	Tên chỉ số	Tên ký hiệu
I	**Nhóm chỉ số đánh giá về tổ chức**	**VNO**
1	Chức năng, nhiệm vụ	VNO-1
2	Đối tượng phục vụ	VNO-2
3	Quyền hạn	VNO-3
4	Trách nhiệm	VNO-4
5	Danh mục các hoạt động nghiệp vụ	VNO-5
6	Quy chế hoạt động	VNO-7
II	**Nhóm chỉ số đánh giá về con người**	**VNH**
7	Quy tắc ứng xử	VNH-1
8	Phương án dự phòng nhân sự	VNH-2
9	Kết nối- hợp tác	VNH-7
III	**Nhóm chỉ số đánh giá về công cụ**	**VNT**
10	Danh sách nguồn thông tin	VNT-2
11	Kênh thông tin liên lạc không gián đoạn	VNT-3
12	Hệ thống theo dõi sự cố	VNT-4
13	Đảm bảo kết nối Internet ổn định	VNT-5
IV	**Nhóm chỉ số đánh giá về quy trình**	**VNP**
14	Quy trình báo cáo sự cố lên cấp quản lý cao hơn	VNP-1
15	Quy trình đánh giá hoàn thiện tổ chức	VNP-7
16	Quy trình tiếp cận khẩn cấp	VNP-8
17	Quy trình xử lý thông tin mật	VNP-9
18	Quy trình kết nối cơ quan quản lý nhà nước	VNP-12
V	**Nhóm chỉ số đánh giá hoạt động thường xuyên**	**VNA**
19	Kế hoạch hoạt động	VNA-1
20	Tham gia nền tảng IRLab	VNA-2
21	Diễn tập thực chiến	VNA-5
22	Chia sẻ thông tin	VNA-6

Bảng điểm đánh giá giai đoạn 1:

STT	Tên chỉ số	Các mức đánh giá (số điểm tối thiểu cần đạt được)		
		Ý tưởng	Sơ khởi	Cơ bản
1	VNO-1	<2	2	3
2	VNO-2	<2	2	3
3	VNO-3	<2	2	3
4	VNO-4	<2	2	3
5	VNO-5	<2	2	3
6	VNO-7	<2	2	3
Tổng theo chỉ số		**<12**	**12**	**18**
7	VNH-1	<1	1	2
8	VNH-2	<1	1	2
9	VNH-7	<1	1	2
Tổng theo chỉ số		**<3**	**3**	**6**
10	VNT-2	<1	1	1
11	VNT-3	<1	1	1
12	VNT-4	0	0	1
13	VNT-5	<1	1	1
Tổng theo chỉ số		**<3**	**3**	**4**
14	VNP-1	0	1	3
15	VNP-7	0	0	2
16	VNP-8	0	0	2
17	VNP-9	0	0	2
18	VNP-12	0	0	2
Tổng theo chỉ số		**<1**	**1**	**11**
19	VNA-1	0	1	2
20	VNA-2	0	1	2
21	VNA-5	0	1	2
22	VNA-6	0	1	2
Tổng theo chỉ số		**<4**	**4**	**8**
Tổng cộng theo mức xếp hạng trưởng thành		**<23**	**23**	**47**

Phụ lục II

MÔ HÌNH ĐÁNH GIÁ MỨC ĐỘ TRƯỞNG THÀNH CỦA CSIRT TẠI VIỆT NAM GIAI ĐOẠN 2

Giai đoạn 2 thực hiện đánh giá mức độ trưởng thành của CSIRT dựa trên ***38 chỉ số*** sau:

STT	Tên chỉ số	Tên ký hiệu
I	**Nhóm chỉ số đánh giá về tổ chức**	**VNO**
1	Chức năng, nhiệm vụ	VNO-1
2	Đối tượng phục vụ	VNO-2
3	Quyền hạn	VNO-3
4	Trách nhiệm	VNO-4
5	Danh mục các hoạt động nghiệp vụ	VNO-5
6	Phân loại sự cố	VNO-6
7	Quy chế hoạt động	VNO-7
8	Chính sách bảo mật	VNO-8
II	**Nhóm chỉ số đánh giá về con người**	**VNH**
9	Quy tắc ứng xử	VNH-1
10	Phương án dự phòng nhân sự	VNH-2
11	Yêu cầu về kỹ năng	VNH-3
12	Phát triển đội ngũ	VNH-4
13	Đào tạo kỹ thuật	VNH-5
14	Đào tạo kỹ năng mềm	VNH-6
15	Kết nối- hợp tác	VNH-7
III	**Nhóm chỉ số đánh giá về công cụ**	**VNT**
16	Danh sách nguồn thông tin	VNT-2
17	Kênh thông tin liên lạc không gián đoạn	VNT-3
18	Hệ thống theo dõi sự cố	VNT-4
19	Đảm bảo kết nối Internet ổn định	VNT-5
IV	**Nhóm chỉ số đánh giá về quy trình**	**VNP**
20	Quy trình báo cáo sự cố lên cấp quản lý cao hơn	VNP-1
21	Quy trình công khai thông tin	VNP-2
22	Quy trình cung cấp thông tin cho cơ quan pháp lý	VNP-3
23	Quy trình phòng ngừa sự cố	VNP-4

24	Quy trình phát hiện sự cố	VNP-5
25	Quy trình xử lý sự cố	VNP-6
26	Quy trình đánh giá hoàn thiện tổ chức	VNP-7
27	Quy trình tiếp cận khẩn cấp	VNP-8
28	Quy trình xử lý thông tin mật	VNP-9
29	Quy trình quản lý nguồn tin	VNP-10
30	Quy trình tiếp cận khách hàng, đối tác	VNP-11
31	Quy trình kết nối cơ quan quản lý nhà nước	VNP-12
32	Quy trình thống kê sự cố	VNP-13
V	**Nhóm chỉ số đánh giá hoạt động thường xuyên**	**VNA**
33	Kế hoạch hoạt động	VNA-1
34	Tham gia nền tảng IRLab	VNA-2
35	Rà quét lỗ hổng	VNA-3
36	Săn lùng mối nguy	VNA-4
37	Diễn tập thực chiến	VNA-5
38	Chia sẻ thông tin	VNA-6

Bảng điểm đánh giá giai đoạn 2:

STT	Tên chỉ số	Các mức đánh giá (số điểm tối thiểu cần đạt được)			
		Ý tưởng	Sơ khởi	Cơ bản	Phát triển
1	VNO-1	<2	2	3	4
2	VNO-2	<2	2	3	4
3	VNO-3	<2	2	3	4
4	VNO-4	<2	2	3	4
5	VNO-5	<2	2	3	4
6	VNO-6	<1	1	1	2
7	VNO-7	<2	2	3	3
8	VNO-8	<1	1	1	2
Tổng theo chỉ số		**<14**	**14**	**20**	**27**
9	VNH-1	<1	1	2	3
10	VNH-2	<1	1	2	3
11	VNH-3	<1	1	1	2
12	VNH-4	<1	1	1	2
13	VNH-5	<1	1	1	2
14	VNH-6	<1	1	1	2

15	VNH-7	<1	1	2	3
Tổng theo chỉ số		**<7**	**7**	**10**	**17**
16	VNT-2	<1	1	1	2
17	VNT-3	<1	1	1	2
18	VNT-4	0	0	1	2
19	VNT-5	<1	1	1	2
Tổng theo chỉ số		**<3**	**3**	**4**	**8**
20	VNP-1	0	1	3	3
21	VNP-2	0	0	1	2
22	VNP-3	0	0	1	2
23	VNP-4	0	0	1	2
24	VNP-5	0	0	1	2
25	VNP-6	0	0	1	2
26	VNP-7	0	0	2	3
27	VNP-8	0	0	2	3
28	VNP-9	0	0	2	3
29	VNP-10	0	0	1	2
30	VNP-11	0	0	1	2
31	VNP-12	0	0	2	3
32	VNP-13	0	0	1	2
Tổng theo chỉ số		**<1**	**1**	**19**	**31**
33	VNA-1	0	1	2	3
34	VNA-2	0	1	2	3
35	VNA-3	0	1	2	3
36	VNA-4	0	1	2	3
37	VNA-5	0	1	2	3
38	VNA-6	0	1	2	3
Tổng theo chỉ số		**<6**	**6**	**12**	**18**
Tổng cộng theo mức xếp hạng trưởng thành		**<31**	**31**	**65**	**101**

Phụ lục III

MÔ HÌNH ĐÁNH GIÁ MỨC ĐỘ TRƯỞNG THÀNH CỦA CSIRT TẠI VIỆT NAM GIAI ĐOẠN 3

Giai đoạn 3 áp dụng nguyên vẹn 44 chỉ số của Mô hình đánh giá.

Bảng điểm đánh giá giai đoạn 3:

STT	Tên chỉ số	Các mức đánh giá (số điểm tối thiểu cần đạt được)				
		Ý tưởng	Sơ khởi	Cơ bản	Phát triển	Tối ưu
1	VNO-1	<2	2	3	4	4
2	VNO-2	<2	2	3	4	4
3	VNO-3	<2	2	3	4	4
4	VNO-4	<2	2	3	4	4
5	VNO-5	<2	2	3	4	4
6	VNO-6	<1	1	1	2	3
7	VNO-7	<2	2	3	3	3
8	VNO-8	<1	1	1	2	3
Tổng theo chỉ số		**<14**	**14**	**20**	**27**	**29**
9	VNH-1	<1	1	2	3	3
10	VNH-2	<1	1	2	3	3
11	VNH-3	<1	1	1	2	3
12	VNH-4	<1	1	1	2	3
13	VNH-5	<1	1	1	2	3
14	VNH-6	<1	1	1	2	3
15	VNH-7	<1	1	2	3	3
Tổng theo chỉ số		**<7**	**7**	**10**	**17**	**21**
16	VNT-1	<1	1	1	1	1
17	VNT-2	<1	1	1	2	3
18	VNT-3	<1	1	1	2	3
19	VNT-4	0	0	1	2	3
20	VNT-5	<1	1	1	2	3
21	VNT-6	0	0	1	1	1
22	VNT-7	0	0	1	1	1
23	VNT-8	0	0	1	1	2

Tổng theo chỉ số		<4	4	8	12	17
24	VNP-1	0	1	3	3	3
25	VNP-2	0	0	1	2	3
26	VNP-3	0	0	1	2	3
27	VNP-4	0	0	1	2	2
28	VNP-5	0	0	1	2	2
29	VNP-6	0	0	1	2	2
30	VNP-7	0	0	2	3	4
31	VNP-8	0	0	2	3	3
32	VNP-9	0	0	2	3	3
33	VNP-10	0	0	1	2	3
34	VNP-11	0	0	1	2	3
35	VNP-12	0	0	2	3	4
36	VNP-13	0	0	1	2	3
37	VNP-14	0	0	1	1	2
38	VNP-15	0	1	1	1	2
Tổng theo chỉ số		**<2**	**2**	**21**	**33**	**42**
39	VNA-1	0	1	2	3	4
40	VNA-2	0	1	2	3	4
41	VNA-3	0	1	2	3	4
42	VNA-4	0	1	2	3	4
43	VNA-5	0	1	2	3	4
44	VNA-6	0	1	2	3	4
Tổng theo chỉ số		**<6**	**6**	**12**	**18**	**24**
Tổng cộng theo mức xếp hạng trưởng thành		**<33**	**33**	**71**	**107**	**133**