Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

1.1. Giới thiệu chung

- Tên dự toán mua sắm: Kiểm tra đánh giá an toàn thông tại Trung tâm Tích hợp dữ liệu tỉnh.
- Chủ đầu tư: Trung tâm Công nghệ Thông tin và Truyền thông tỉnh Quảng Ninh.
- Tên gói thầu: Gói thầu số 03: Kiểm tra đánh giá an toàn thông tin tại Trung tâm THDL tỉnh.
- Tóm tắt công việc chính của gói thầu: Thực hiện kiểm tra đánh giá an toàn thông tin các hệ thống được phê duyệt cấp độ 3 tại Trung tâm Tích hợp dữ liệu tỉnh: Hệ thống Cổng thông tin điện tử, Hệ thống Chính quyền điện tử, Hệ thống cơ sở hạ tầng kỹ thuật dùng chung tại Trung tâm Tích hợp dữ liệu.
- Địa điểm kiểm tra, đánh giá: Trung tâm Tích hợp dữ liệu tầng 4, tòa nhà VNPT, số 1 phường Hồng Gai, Quảng Ninh.
- Nguồn vốn: Ngân sách nhà nước tỉnh năm 2025 được cấp tại Quyết định số 1431/QĐ-UBND ngày 12/5/2025 của UBND tỉnh Quảng Ninh; số 121/QĐ-SKHCN ngày 29/5/2025 của Sở Khoa học và Công nghệ.
- Hình thức lựa chọn nhà thầu: Chào hàng cạnh tranh trong nước, qua mạng.
- Phương thức đấu thầu: Một giai đoạn, một túi hồ sơ.
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý IV/2025.
- Loại hợp đồng: Trọn gói.
- Thời gian thực hiện gói thầu: 60 ngày

1.2. Quy mô cung cấp dịch vụ của gói thầu

STT	Tiêu chí, nội dung đánh giá
I	**KIỂM TRA ĐÁNH GIÁ AN TOÀN THÔNG TIN CHO TRUNG TÂM TTDL**
1	**Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ**
1.1	***Kiểm tra, đánh giá tuân thủ đối với Chủ quản hệ thống thông tin theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP, gồm:***
1.1.1	Việc thực hiện thành lập/chỉ định đơn vị chuyên trách/bộ phận chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 20 Nghị định 85/2016/NĐ-CP
1.1.2	Việc thực hiện lập Hồ sơ đề xuất cấp độ, tổ chức thẩm định, phê duyệt Hồ sơ đề xuất cấp độ theo quy định đối với các hệ thống thông tin thuộc phạm vi quản lý

STT	Tiêu chí, nội dung đánh giá
1.1.3	Việc triển khai phương án bảo đảm an toàn thông tin theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt đối với các hệ thống thông tin thuộc phạm vi quản lý
1.1.4	Việc tổ chức thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin trong phạm vi cơ quan, tổ chức mình theo quy định tại điểm c khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP
1.1.5	Việc tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về an toàn thông tin theo quy định tại điểm d Khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP
1.2	***Kiểm tra, đánh giá tuân thủ đối với Đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP, gồm:***
1.2.1	Công tác tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin;
1.2.2	Công tác thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với Hồ sơ đề xuất cấp độ theo thẩm quyền quy định đối với đơn vị chuyên trách về an toàn thông tin
1.3	***Kiểm tra, đánh giá việc tổ chức thực thi các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt đối với các đơn vị vận hành***
2	**Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin theo HSĐXCĐ được phê duyệt**
2.1	***Đánh giá Quy chế bao gồm đầy đủ các quy định và quy trình đáp ứng các yêu cầu về quản lý được quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930-2017***
2.1.1	Các quy định trong Quy chế
a)	Thiết lập chính sách an toàn thông tin
b)	Tổ chức bảo đảm an toàn thông tin
c)	Bảo đảm nguồn nhân lực
d)	Quản lý thiết kế, xây dựng hệ thống
đ)	Quản lý vận hành hệ thống
2.1.2	Các quy trình kèm theo Quy chế
a)	Quy trình tuyển dụng cán bộ
b)	Quy trình chấm dứt hoặc thay đổi công việc
c)	Quy trình thử nghiệm và nghiệm thu hệ thống
d)	Quản lý an toàn mạng
đ)	Quản lý an toàn máy chủ và ứng dụng

STT	Tiêu chí, nội dung đánh giá
e)	Quản lý an toàn dữ liệu
g)	Quản lý an toàn thiết bị đầu cuối
h)	Quản lý phòng chống phần mềm độc hại
i)	Quản lý giám sát an toàn hệ thống thông tin
k)	Quản lý điểm yếu an toàn thông tin
l)	Quản lý sự cố an toàn thông tin
m)	Quản lý an toàn người sử dụng đầu cuối
n)	Quản lý rủi ro an toàn thông tin
o)	Kết thúc vận hành, khai thác, thanh lý, hủy bỏ
2.2	***Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin***
	Đánh giá Đơn vị vận hành có nhật ký quản lý vận hành hệ thống theo các quy định và quy trình ban hành theo Quy chế bảo đảm an toàn thông tin
	Báo cáo đánh giá tuân thủ yêu cầu phải có các tài liệu minh chứng hệ thống được quản lý, vận hành theo Quy chế được ban hành là nhật kỷ vận hành hệ thống
2.3	***Đánh giá việc thiết kế hệ thống theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt***
	Báo cáo đánh giá tuân thủ yêu cầu có sơ đồ vật lý, sơ đồ logic
	Báo cáo đánh giá có minh chứng cấu hình trên thiết bị hệ thống để chứng minh hệ thống được thiết kế đúng theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ
2.4	***Đánh giá việc thiết lập, cấu hình hệ thống theo phương án trong Hồ sơ đề xuất cấp độ được phê duyệt (kèm minh chứng) được quy định tại Điều 12 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017***
	Thiết bị hệ thống
	Máy chủ
	Ứng dụng
	Dữ liệu
3	**Kiểm tra đánh giá phát hiện mã độc, lỗ hổng bảo mật, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin**
3.1	Đánh giá an toàn thông tin cho thiết bị hệ thống
a)	Thiết bị mạng lớp 2: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình log, giám sát.

STT	Tiêu chí, nội dung đánh giá
b)	Thiết bị mạng lớp 3: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình log, giám sát; Kiểm tra, đánh giá cấu hình định tuyến (thiết bị mạng)
c)	Thiết bị bảo mật: Đánh giá vai trò thiết bị trong hệ thống; Kiểm tra, đánh giá cấu hình lớp an ninh; Kiểm tra, đánh giá cấu hình quản trị; Kiểm tra, đánh giá cấu hình chung: phiên bản, lỗ hổng của thiết bị; Kiểm tra, đánh giá cấu hình chính sách tài khoản; Kiểm tra chính sách kết nối quản trị; Kiểm tra cấu hình log, giám sát; Kiểm tra, đánh giá cấu hình định tuyến; Kiểm tra chính sách, cấu hình ngăn chặn tấn công trên thiết bị
3.2	Đánh giá an toàn thông tin cho máy chủ
	- Kiểm tra bản vá và cập nhật hệ điều hành - Kiểm tra cấu hình hệ điều hành - Kiểm tra cấu hình chứng thực - Kiểm tra cấu hình log, giám sát - Kiểm tra các cấu hình chính sách nội bộ - Kiểm tra, đánh giá cấu hình chính sách tài khoản - Kiểm tra chính sách kết nối quản trị - Kiểm tra các giải pháp về phòng, chống mã độc - Các tiêu chí khác theo CIS Server Benchmark
3.3	Đánh giá an toàn thông tin cho ứng dụng
	- Kiểm tra tính an toàn của các thư viện mã nguồn - Kiểm tra, đánh giá Quản lý cấu hình & triển khai - Kiểm tra, đánh giá Quản lý định danh - Kiểm tra, đánh giá Xác thực - Kiểm tra, đánh giá Phân quyền - Kiểm tra, đánh giá Quản lý phiên - Kiểm tra, đánh giá Sàng lọc dữ liệu đầu vào - Kiểm tra, đánh giá Cơ chế xử lý lỗi - Kiểm tra, đánh giá Thuật toán mã hóa - Kiểm tra, đánh giá Logic nghiệp vụ - Kiểm tra Xử lý phía người dùng - Kiểm tra, đánh giá khả năng tồn tại các lỗ hổng overflows, SQL Injection, Race Conditions
II	**KIỂM TRA ĐÁNH GIÁ HẠ TẦNG KỸ THUẬT**
	Kiểm tra đánh giá các hệ thống:

STT	Tiêu chí, nội dung đánh giá
	Kiểm tra vị trí vật lý của Trung tâm THDL (Kiểm tra tổng thể hệ thống các buồng, phòng thuộc Trung tâm tích hợp dữ liệu tỉnh đảm bảo yêu cầu theo chỉ thị 02/CT-TTg ngày 04/07/2018 của Thủ tướng Chính phủ về công tác bảo vệ Bí mật nhà nước trên không gian mạng). - Kiểm tra hệ thống kiểm soát truy cập vật lý. - Kiểm tra các hệ thống chống trộm, phá hoại. - Kiểm tra hệ thống chống sét. - Kiểm tra hệ thống chống cháy. - Kiểm tra hệ thống chống ẩm, chống thấm. - Kiểm tra hệ thống kiểm soát nhiệt độ và độ ẩm. - Kiểm tra hệ thống nguồn cung cấp. - Phân tích, đánh giá, tổng hợp và đưa ra báo cáo
1	Hệ thống Camera giám sát (Bao gồm máy chủ lưu trữ và quản trị hệ thống Camera, các camera)
2	Hệ thống quản trị tập trung sitescan web (Bao gồm phần mềm quản trị tập trung sitescan Liebert/Emerson, các phần tử kết nối như máy phát điện, UPS, Điều hoà chính xác, hệ thống phát hiện chất lỏng..)
3	Hệ thống Access control (Bao gồm Máy chủ quản trị, 06 bộ cửa đóng mở bằng sinh trắc học (vân tay, cửa từ...)
4	Hệ thống điện
	Trạm biến áp công suất 630kVA
	Máy phát điện Himoinsa 670 kVA
	Hệ thống tủ phân phối ATS&MSB
	Hệ thống lưu điện UPS Emerson 100kVA và ắc quy
5	Hệ thống điều hòa
6	Hệ thống Phòng cháy, chữa cháy

1.3. Phạm vi cung cấp dịch vụ của gói thầu

1.3.1. Danh sách ứng dụng, thiết bị hệ thống, máy chủ

STT	Tên thiết bị/ Chủng loại	Đơn vị tính	Số lượng
I	**ỨNG DỤNG**		
1	Cổng thông tin điện tử tỉnh Quảng Ninh: https://www.quangninh.gov.vn	Hệ thống	1
2	Hệ thống Chính quyền điện tử tỉnh Quảng Ninh	Hệ thống	1
II	**THIẾT BỊ TRONG HỆ THỐNG**		**111**
Thiết bị mạng bảo mật			**37**
1	Router Juniper MX5	Bộ	3

STT	Tên thiết bị/ Chủng loại	Đơn vị tính	Số lượng
2	INTERNET-RT /Cisco ASR1001-X	Bộ	1
3	Firewall SRX650	Bộ	2
4	Switch Juniper EX2200-24T-4G	Bộ	3
5	Internet-SW Cisco C9300- 48T-A	Bộ	1
6	Thiết bị INT-Load BL Big IP F5 3900	Bộ	1
7	Core Switch Juniper EX8208 Ethernet Switch	Bộ	2
8	HPE 12904E Spine Switch	Bộ	2
9	Leaf Switch HPE FlexFabric 5940 Switch (JH398A)	Bộ	2
10	Leaf Switch HPE FlexFabric 5940 Switch (JH397A)	Bộ	2
11	SRV-FW Checkpoint Firewall Appliance 12400	Bộ	2
12	ACC-SW Switch Juniper EX4200-48T	Bộ	4
13	Thiết bị SRV-Load BL-01/ Big IP F5 2200S	Bộ	2
14	FW-DB-01/ Firewall Imperva X2520	Bộ	1
15	Firewall Juniper SRX4200	Bộ	2
16	SW Monitor/Juniper EX2200-48T-4G	Bộ	1
17	Cặp Thiết bị SSL VPN Juniper MAG6611 Junos Pulse Gateway – SSL VPN Device	Bộ	1
18	Imperva SecureSphere Management Appliance M120	Bộ	1
19	Check Point Smart-1 Appliance – Checkpoint Security Management Device	Bộ	1
20	Juniper Security NSMXpress Appliance	Bộ	1
21	Switch Cisco Catalyst 2960-24	Bộ	1
22	Switch Cisco SG300-28	Bộ	1
Thiết bị lưu trữ, sao lưu			**9**
23	HP 3Par7400	Bộ	1
24	HP 3Par8400	Bộ	1
25	HP MSL2024	Bộ	1
26	HP MSL4048	Bộ	1
27	HP StoreOne 3100	Bộ	1
28	HP StoreOne 5500	Bộ	1
29	HP 3Par8440	Bộ	1
30	HP MSL4048	Bộ	1
31	HPE StoreEasy 1660	Bộ	1
Máy chủ Host			**52**
32	Máy chủ Host thành phố thông minh	Bộ	48

STT	Tên thiết bị/ Chủng loại	Đơn vị tính	Số lượng
33	Máy chủ quản trị hệ thống máy chủ thành phố Thông minh	Bộ	4
Máy chủ Rack			**13**
34	DB SERVER/ HP DL580G7	Bộ	6
35	DB SERVER/ HP DL380G9	Bộ	4
36	APP SERVER/ HP DL360G10	Bộ	1
37	DB SERVER/ HPE DL580G9	Bộ	2
III.	**MÁY CHỦ TRONG HỆ THỐNG**		**41**
1	Máy chủ Web01 cài đặt Windows Server 2012	Bộ	1
2	Máy chủ Web02 cài đặt Windows Server 2012	Bộ	1
3	Máy chủ Server App01 cài đặt Windows Server 2012	Bộ	1
4	Máy chủ CBCC03 cài đặt Window Server 2016	Bộ	1
5	Máy chủ CBCC04 cài đặt Window Server 2016	Bộ	1
6	Máy chủ CBCC05 cài đặt Window Server 2016	Bộ	1
7	Máy chủ CBCC06 cài đặt Window Server 2016	Bộ	1
8	Máy chủ QLHCT-APP01 cài đặt Window Server 2012	Bộ	1
9	Máy chủ QLHCT-APP02 cài đặt Window Server 2012	Bộ	1
10	Máy chủ QLHCT-APP03 cài đặt Window Server 2012	Bộ	1
11	Máy chủ QLVB-APP01 cài đặt Window Server 2012	Bộ	1
12	Máy chủ QLVB-APP02 cài đặt Window Server 2012	Bộ	1
13	Máy chủ QLVB-APP04 cài đặt Window Server 2016	Bộ	1
14	Máy chủ QLVB-APP05 cài đặt Window Server 2016	Bộ	1
15	Máy chủ QLVB-APP06 cài đặt Window Server 2016	Bộ	1
16	Máy chủ QLVB-APP07 cài đặt Window Server 2016	Bộ	1
17	Máy chủ QLXD cài đặt Window Server 2012	Bộ	1
18	Máy chủ QLDD cài đặt Window Server 2012	Bộ	1
19	Máy chủ QLĐT cài đặt Window Server 2012	Bộ	1
20	Máy chủ QLDL cài đặt Window Server 2012	Bộ	1
21	Máy chủ QLMT cài đặt Window Server 2012	Bộ	1
22	Máy chủ QLHCS cài đặt Window Server 2012	Bộ	1
23	Máy chủ QLHN cài đặt Window Server 2012	Bộ	1
24	Máy chủ QHHDND cài đặt Window Server 2012	Bộ	1
25	Máy chủ QLYD cài đặt Window Server 2019	Bộ	1
26	Máy chủ WEB41 cài đặt Window Server 2012	Bộ	1
27	Máy chủ WEB42 cài đặt Window Server 2012	Bộ	1

STT	Tên thiết bị/ Chủng loại	Đơn vị tính	Số lượng
28	Máy chủ BI01 cài đặt Window Server 2012	Bộ	1
29	Máy chủ BI02 cài đặt Window Server 2012	Bộ	1
30	Máy chủ ETL01 cài đặt Window Server 2012	Bộ	1
31	Máy chủ ETL02 cài đặt Window Server 2012	Bộ	1
32	Máy chủ DVLT 01 cài đặt Window Server 2016	Bộ	1
33	Máy chủ DVLT 02 cài đặt Window Server 2016	Bộ	1
34	Máy chủ DVLT 03 cài đặt Window Server 2016	Bộ	1
35	Máy chủ BPM01 cài đặt Window Server 2012	Bộ	1
36	Máy chủ BPM02 cài đặt Window Server 2012	Bộ	1
37	Máy chủ EMS01 cài đặt Window Server 2012	Bộ	1
38	Máy chủ EMS02 cài đặt Window Server 2012	Bộ	1
39	Máy chủ ESB 01 cài đặt Window Server 2012	Bộ	1
40	Máy chủ ESB 02 cài đặt Window Server 2012	Bộ	1
41	Máy chủ LTVBCP cài đặt Ubutu	Bộ	1

1.3.2. Danh sách thiết bị, hệ thống hạ tầng kỹ thuật

STT	Hệ thống, thiết bị	Ghi chú	Số lượng
1	Hệ thống Camera giám sát (Bao gồm máy chủ lưu trữ và quản trị hệ thống Camera, 13 camera)		01
2	Hệ thống quản trị tập trung sitescan web (Bao gồm phần mềm quản trị tập trung sitescan Liebert/Emerson, các phần tử kết nối như máy phát điện, UPS, Điều hoà chính xác, hệ thống phát hiện chất lỏng..)		01
3	Hệ thống Access control (Bao gồm Máy chủ quản trị, 06 bộ cửa đóng mở bằng sinh trắc học (vân tay, cửa từ…)		01
4	Hệ thống điện	Trạm biến áp công suất 630kVA	01
		Máy phát điện Himoinsa 670 kVA	01
		Hệ thống tủ phân phối ATS&MSB	01

STT	Hệ thống, thiết bị	Ghi chú	Số lượng
		Hệ thống lưu điện UPS Emerson 100kVA và ắc quy.	01
5	Hệ thống điều hòa	Điều hòa chính xác: 04 hệ thống Liebert P2060DA; 01 hệ thống Liebert PEX+2060DA	05
6	Hệ thống Phòng cháy, chữa cháy	Hệ thống chữa cháy tự động FM-200	01

2. Mục tiêu công việc

2.1. Mục đích

- Đảm bảo Trung tâm Tích hợp dữ liệu tỉnh (TTTHDL) và các hệ thống thông tin trọng yếu của tỉnh Quảng Ninh hoạt động ổn định, an toàn, đảm bảo về bảo mật và toàn vẹn dữ liệu; thực hiện kiểm tra đánh giá ATTT các hệ thống nhằm xác định tính hiệu quả các hệ thống, mức độ đảm bảo ATTT đáp ứng các mục tiêu về an toàn an ninh, từ đó đưa ra các phương án, quy trình để bảo vệ hệ thống một cách tốt nhất trước những nguy cơ về lỗ hổng và nguy cơ tấn công.

- Thông qua việc kiểm tra đánh đánh giá an toàn thông tin hệ thống để kịp thời khắc phục những hạn chế, cải thiện hệ thống, giảm thiểu các rủi ro đối với hệ thống có thể xảy ra thực tế trong việc quản lý, vận hành, khai thác, sử dụng các hệ thống thông tin của tỉnh.

2.2. Yêu cầu

- Việc kiểm tra đánh giá ATTT hệ thống cũng là thước đo mức độ an toàn của hệ thống của tỉnh, cần đảm bảo các bước như: Rà soát, kiểm tra, kiểm thử hệ thống. Đảm bảo việc kiểm tra đánh giá theo 03 hình thức: đánh giá từ bên ngoài (Black - Box); đánh giá từ bên trong (White - Box), đánh giá hộp xám (Gray - Box).

- Trong quá trình kiểm tra, đánh giá cần đảm bảo không ảnh hưởng đến các hệ thống đang hoạt động, đảm bảo an toàn thông tin, bảo mật thông tin trong quá trình triển khai đánh giá.

- Kiểm tra đánh giá ATTT cho Trung tâm Tích hợp dữ liệu tỉnh và Hệ thống Chính quyền điện tử theo đúng quy định, đảm bảo tiêu chuẩn TCVN-11930:2017 và các yêu cầu tại Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 và các yêu cầu của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về đảm bảo an toàn hệ thống thông tin theo cấp độ.

- Có báo cáo đánh giá cụ thể các nội dung và đề ra phương án, giải pháp thực hiện khắc phục và triển khai thực hiện khắc phục.

3. Yêu cầu kỹ thuật của gói thầu

Kiểm tra, đánh giá ATTT cho các hệ thống thông tin dùng chung được phê duyệt cấp độ 3 tại TTTHDL tỉnh (Quyết định số 1501/QĐ-UBND ngày 24/4/2024 của UBND tỉnh Quảng Ninh) theo quy định của pháp luật tại Nghị định 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT và hướng dẫn của Bộ Thông tin và Truyền thông (*trước hợp*

nhất với Bộ Khoa học và Công nghệ) tại Công văn 2596/BTTTT-CATTT ngày 02/7/2024 cho các hệ thống được phê duyệt cấp độ 3 tại TTTHDL tỉnh, bao gồm các nội dung:

3.1. Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ

Phạm vi đánh giá:

a) Kiểm tra, đánh giá tuân thủ đối với chủ quản hệ thống thông tin theo quy định tại Điều 20 Nghị định 85/2016/NĐ-CP.

b) Kiểm tra, đánh giá tuân thủ đối với đơn vị chuyên trách về ATTT của chủ quản hệ thống thông tin theo quy định tại Điều 21 Nghị định 85/2016/NĐ-CP.

c) Kiểm tra, đánh giá tuân thủ đối với đơn vị vận hành theo quy định tại Điều 22 Nghị định 85/2016/NĐ-CP.

d) Kiểm tra, đánh giá việc tổ chức thực thi các biện pháp bảo đảm ATTT theo phương án bảo đảm ATTT được phê duyệt đối với các đơn vị vận hành.

Nội dung đánh giá:

a) Việc thực hiện thành lập/chỉ định đơn vị chuyên trách/bộ phận chuyên trách về ATTT của chủ quản hệ thống thông tin theo quy định tại khoản 1 Điều 20 Nghị định 85/2016/NĐ-CP.

b) Việc thực hiện lập Hồ sơ đề xuất cấp độ (HSĐXCĐ), tổ chức thẩm định, phê duyệt HSĐXCĐ theo quy định đối với các hệ thống thông tin thuộc phạm vi quản lý.

c) Việc triển khai phương án bảo đảm ATTT theo phương án trong HSĐXCĐ được phê duyệt đối với các hệ thống thông tin thuộc phạm vi quản lý.

d) Việc tổ chức thực hiện kiểm tra, đánh giá ATTT và quản lý rủi ro ATTT trong phạm vi cơ quan, tổ chức mình theo quy định tại điểm c Khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP.

đ) Việc tổ chức thực hiện đào tạo ngắn hạn, tuyên truyền, phổ biến, nâng cao nhận thức và diễn tập về ATTT theo quy định tại điểm d Khoản 2 Điều 20 Nghị định 85/2016/NĐ-CP.

e) Công tác tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, giám sát công tác bảo đảm ATTT; Công tác thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với HSĐXCĐ theo thẩm quyền quy định đối với đơn vị chuyên trách về ATTT.

g) Kiểm tra, đánh giá việc tổ chức thực thi các biện pháp bảo đảm ATTT theo phương án bảo đảm ATTT được phê duyệt đối với các đơn vị vận hành.

h) Kiểm tra, đánh giá tuân thủ đối với Đơn vị vận hành theo quy định tại Điều 22, NĐ85/2016/NĐ-CP.

3.2. Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm ATTT theo phương án bảo đảm ATTT theo HSĐXCĐ được phê duyệt.

Phạm vi đánh giá:

Kiểm tra, đánh giá hiệu quả của việc triển khai các biện pháp quản lý và kỹ thuật bảo đảm ATTT theo phương án được phê duyệt trong HSĐXCĐ của TTTHDL tỉnh.

<u>Nội dung đánh giá:</u>

a) Đánh giá Quy chế bao gồm đầy đủ các quy định và quy trình đáp ứng các yêu cầu về quản lý được quy định tại Điều 9, Điều 10 Thông tư 12/2022/TT-BTTTT

b) Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm ATTT trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin.

c) Đánh giá việc thiết kế hệ thống theo phương án được phê duyệt trong HSĐXCĐ.

d) Đánh giá việc thiết lập, cấu hình hệ thống theo phương án trong HSĐXCĐ được phê duyệt (*Đối với từng thiết bị hệ thống, máy chủ, ứng dụng và dữ liệu quy định tại Điểm 1.3.1, Khoản 1.3, Mục 1 Chương V của E-HSMT theo các quy định tại Điều 12 Thông tư 12/2022/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 và kèm minh chứng*).

đ) Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hành, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống theo hướng dẫn của Bộ Thông tin và Truyền thông (*trước hợp nhất với Bộ Khoa học và Công nghệ*).

3.3. Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng bảo mật, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin

3.3.1. Phạm vi, đối tượng đánh giá

Phạm vi cung cấp dịch vụ kiểm tra, đánh giá, rà quét, phát hiện mã độc, lỗ hổng bảo mật, điểm yếu, kiểm thử xâm nhập hệ thống toàn bộ thành phần trong hệ thống (*đối với từng thiết bị hệ thống, máy chủ và ứng dụng quy định tại Điểm 1.3.1, Khoản 1.3, Mục 1 Chương V của E-HSMT*).

3.3.2. Nội dung đánh giá

- Đánh giá an toàn thông tin cho thiết bị hệ thống
- Đánh giá an toàn thông tin cho máy chủ
- Đánh giá an toàn thông tin cho ứng dụng

3.3.3. Phương pháp kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin

Kiểm tra đánh giá theo 03 hình thức: đánh giá từ bên ngoài (Black - Box); đánh giá từ bên trong (White - Box), đánh giá hộp xám (Gray - Box).

i. Kiểm tra, đánh giá hộp đen (Black box):

Người đánh giá phải thực hiện việc kiểm tra, đánh giá hệ thống từ bên ngoài, không được cung cấp bất kỳ thông tin nội bộ nào liên quan đến hệ thống: nền tảng hệ thống, phiên bản ứng dụng, sơ đồ kiến trúc, tài khoản đăng nhập, mã nguồn,… Quá trình đánh giá phải được tiến hành theo phương thức mô phỏng một cuộc tấn công từ bên ngoài, chỉ sử dụng các thông tin công khai để thu thập, phân tích và khai thác.

ii. Kiểm tra, đánh giá hộp xám (Gray box):

Người đánh giá sẽ được cung cấp một số thông tin nội bộ của hệ thống: sơ đồ mạng, kiến trúc hệ thống, tài khoản người dùng thông thường hoặc một phần mã nguồn,… để phục vụ cho quá trình kiểm tra, đánh giá. Việc đánh giá phải được thực hiện theo phương thức mô phỏng kịch bản tấn công từ phía người dùng có quyền hạn nhất định trong hệ

thống.

iii. Kiểm tra, đánh giá hộp trắng (White box):

Người đánh giá sẽ được cung cấp đầy đủ thông tin và quyền tiếp cận trực tiếp đối với hệ thống: ứng dụng, mã nguồn, cấu hình, tài liệu thiết kế, sơ đồ mạng và tài khoản quản trị,…nhằm thực hiện việc đánh giá tổng thể, toàn diện và đầy đủ nhất. Quá trình đánh giá phải được tiến hành theo phương thức mô phỏng hiện trạng từ bên trong (tương tự vai trò quản trị hệ thống) bao gồm rà soát mã nguồn, cấu hình bảo mật, nhật ký hệ thống và quản lý tài khoản.

3.4. Kiểm tra đánh giá hạ tầng kỹ thuật

3.4.1. Phạm vi kiểm tra, đánh giá

Kiểm tra đánh giá các hệ thống: Hệ thống Camera giám sát, Hệ thống quản trị tập trung sitescan web, Hệ thống Access control, Hệ thống điện, Hệ thống điều hòa, Hệ thống Phòng cháy, chữa cháy (*đối với từng thiết bị, hệ thống hạ tầng kỹ thuật quy định tại Điểm 1.3.2, Khoản 1.3, Mục 1 Chương V của E-HSMT*).

3.4.2. Nội dung đánh giá

Kiểm tra vị trí vật lý của TTTHDL tỉnh (Kiểm tra tổng thể hệ thống các buồng, phòng thuộc TTTHDL tỉnh đảm bảo yêu cầu theo Chỉ thị 02/CT-TTg ngày 04/07/2018 của Thủ tướng Chính phủ về công tác bảo vệ Bí mật nhà nước trên không gian mạng)

3.5. Yêu cầu đối với tổ chức và nhân sự cung cấp dịch vụ kiểm tra, đánh giá ATTT mạng

3.5.1. Yêu cầu về pháp lý đối với tổ chức cung cấp dịch vụ

- Có giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng do cơ quan có thẩm quyền cấp còn hiệu lực hoặc quyết định giao nhiệm vụ/quyết định quy định chức năng nhiệm vụ được cơ quan nhà nước có thẩm quyền ban hành trong đó có nội dung cho phép nhà thầu cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng.
- Giấy phép/quyết định còn hiệu lực trong thời gian thực hiện dịch vụ

3.5.2. Yêu cầu về năng lực và kinh nghiệm đối với tổ chức cung cấp dịch vụ

- Tổ chức thực hiện dịch vụ phải cam kết đảm bảo bí mật thông tin liên quan đến dịch vụ như: thông tin hệ thống, thông tin kết quả đánh giá.
- Trung thực khi đưa ra các kết quả đánh giá và các khuyến nghị khắc phục.
- Có tối thiểu 01 hợp đồng đã thực hiện về kiểm tra, đánh giá ATTT đối với hệ thống thông tin cấp độ tương đương (cấp độ 3) hoặc cao hơn.
- Tổ chức thực hiện dịch vụ cam kết có đủ nhân sự thực hiện dịch vụ trong đó tối thiểu là 06 chuyên gia, bao gồm 01 chuyên gia loại 1 và 05 chuyên gia loại 2. Nhân sự thực hiện có hợp đồng lao động với nhà thầu và trường hợp sử dụng nhân sự chủ chốt không thuộc quản lý của nhà thầu thì phải nêu rõ lý do.

3.5.3. Yêu cầu đối với Trưởng nhóm (Chuyên gia loại 1) kiểm tra, đánh giá ATTT mạng

- Có các chứng chỉ liên quan đến kiểm tra, đánh giá ATTT: Có ít nhất một trong các chứng chỉ như CEH, CISM, CISSP, Sec+, ECSA, LPT, GSEC, GPEN, GXPN, OSCP, CREST còn hiệu lực.

- Đã chủ trì tối thiểu 01 hợp đồng đã thực hiện về kiểm tra, đánh giá ATTT đối với hệ thống thông tin cấp độ tương đương (cấp độ 3) hoặc cao hơn.

- Đã trực tiếp tham gia thực hiện ít nhất 02 hợp đồng kiểm tra, đánh giá ATTT đối với hệ thống thông tin cấp độ tương đương (cấp độ 3) hoặc cao hơn.

3.5.4. Yêu cầu đối với Chuyên gia (Chuyên gia loại 2) kiểm tra, đánh giá ATTT mạng

- Có các chứng chỉ liên quan đến kiểm tra, đánh giá ATTT: Có ít nhất một trong các chứng chỉ như CEH, CISM, CISSP, CHFI, Sec+, ECSA, LPT, GSEC, GPEN, GXPN, OSCP, CREST còn hiệu lực.

- Đã tham gia tối thiểu 01 hợp đồng kiểm tra, đánh giá ATTT đối với hệ thống thông tin cấp độ tương đương (cấp độ 3) hoặc cao hơn.

3.5.5. Yêu cầu khi cung cấp dịch vụ tại Trung tâm THDL tỉnh:

- Tuân thủ nghiêm ngặt theo các quy trình, quy định về an toàn lao động khi làm việc tại Trung tâm THDL.

- Quá trình làm việc, chuyển giao công nghệ và xử lý nâng cấp, tích hợp, cài đặt các thao tác đối với hệ thống của Trung tâm THDL phải được ghi chép cụ thể vào sổ Nhật ký trực.

- Không được mang, sử dụng các thiết bị điện thoại, máy tính xách tay, máy tính bảng hoặc các thiết bị điện tử cá nhân khác (máy chụp hình, máy quay phim, thiết bị lưu trữ,...) khi vào bên trong Trung tâm THDL, trừ trường hợp có sự đồng ý của lãnh đạo đơn vị trực tiếp quản lý, vận hành Trung tâm THDL.

3.6. Yêu cầu về đảm bảo an toàn, bảo mật thông tin, dữ liệu đối với nhà thầu triển khai

- Thực hiện dịch vụ nhưng không được làm ảnh hưởng tới hoạt động các hệ thống khác của đơn vị.

- Cam kết bảo mật tuyệt đối và chịu trách nhiệm với các thông tin được lưu trữ trên ổ cứng máy chủ của Trung tâm THDL tỉnh khi thực hiện các thao tác kiểm tra đánh giá ATTT.

- Cam kết không thực hiện các phương pháp có nguy cơ làm dừng dịch vụ, gây mất dữ liệu hoặc hỏng hóc hệ thống. Nhà thầu phải chịu trách nhiệm bồi thường thiệt hại và xử lý hậu quả nếu vi phạm cam kết.

- Giữ bí mật thông tin và số liệu liên quan đến sự hoạt động của Trung tâm THDL tỉnh và các đơn vị liên quan đang đặt thiết bị tại Trung tâm THDL tỉnh. Nếu xảy ra sự cố về bảo mật, lộ bí mật thông tin nhà nước của tỉnh Quảng Ninh, Nhà thầu phải hoàn toàn chịu trách nhiệm trước pháp luật.

- Nghiêm cấm sao chép dữ liệu của Trung tâm THDL dưới mọi hình thức.

- Không được mang các thiết bị, vật dụng, vật tư ra khỏi khu vực của Trung tâm THDL.

- Thực hiện một cách chuyên nghiệp, có đầy đủ dụng cụ, thiết bị, máy móc, phần mềm phục vụ triển khai dịch vụ.

- Nhân sự do nhà thầu đề xuất thực hiện phải chấp hành các nội quy, quy định của Trung tâm THDL.

3.7. Báo cáo đánh giá

STT	Tên sản phẩm	Đơn vị tính	Số lượng	
			Bản cứng	Bản mềm
1	Báo cáo kết quả Kiểm tra đánh giá An toàn thông tin tại Trung tâm Tích hợp dữ liệu tỉnh	Báo cáo	02	01

Báo cáo cần tổng hợp kết quả kiểm tra, đánh giá theo từng phương pháp: hộp đen (Black box), hộp xám (Gray box), hộp trắng (White box); lập danh sách các lỗ hổng phát hiện (nếu có) và minh chứng; phân loại theo mức độ cao, trung bình, thấp; mô tả kỹ thuật khai thác từng lỗ hổng (nếu có) và đề xuất biện pháp khắc phục cụ thể như sau:

- Đối với thiết bị, hệ điều hành

+ Đối với lỗi hệ điều hành, thiết bị còn được các nhà cung cấp hỗ trợ: Nhà thầu đưa ra phương án xử lý lỗ hổng, điểm yếu, phương án cấu hình, tăng cường bảo mật và phối hợp các bên liên quan để xử lý, bảo đảm việc nâng cấp, xử lý không ảnh hưởng đến hoạt động của hệ thống.

+ Đối với lỗi hệ điều hành, thiết bị hết hạn hỗ trợ từ nhà cung cấp: Nhà thầu cần đưa ra khuyến nghị gia hạn, nâng cấp và hỗ trợ cấu hình hệ thống, tăng cường bảo mật để giảm thiểu rủi ro.

- Đối với ứng dụng

+ Đối với ứng dụng nội bộ: chỉ ra lỗi và phối hợp với các bên liên quan để xử lý lỗi, và thực hiện kiểm tra lại sau khi lỗi được vá.

+ Đối với ứng dụng không còn hỗ trợ bởi bên phát triển, Nhà thầu cần khuyến nghị và hỗ trợ cấu hình hệ thống, tăng cường bảo mật để giảm thiểu rủ ro.

Nhà thầu thực hiện đánh giá lại sau các nội dung khuyến nghị sau khi chủ đầu tư/các bên liên quan thực hiện sửa lỗi.

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

Trong đó phải nêu rõ danh sách các công cụ, phương pháp sử dụng để triển khai dịch vụ.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Các tài liệu bàn giao sau khi triển khai dịch vụ kiểm tra, đánh giá ATTT mạng

- Tài liệu "Cam kết bảo mật thông tin - NDA" được ký giữa Tổ chức cung cấp dịch vụ và Chủ đầu tư.

- Các biên bản kiểm tra đánh giá các hệ thống tại Trung tâm THDL tỉnh.

- Báo cáo kiểm tra đánh giá hệ thống Chính quyền điện tử và các hệ thống thông tin tại Trung tâm Tích hợp dữ liệu gồm đầy đủ các nội dung:

+ Thể hiện toàn bộ các nội dung đã triển khai thực hiện.

+ Hiệu quả của các biện pháp đảm bảo an toàn thông tin theo phương án đảm bảo an toàn thông tin được phê duyệt.

+ Đưa ra phương án và kế hoạch xử lý lỗ hổng, điểm yếu và phương án cấu hình, tăng cường bảo mật.

+ Các nội dung, phương án cần bổ sung để đáp ứng yêu cầu đảm bảo an toàn hệ thống thông tin đối với hệ thống thông tin cấp độ 3 theo quy định tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông Quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ đối với: Trung tâm tích hợp dữ liệu tỉnh Quảng Ninh; Hệ thống Chính quyền điện tử tỉnh Quảng Ninh.