Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

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

- Tên gói thầu: Kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin mức độ 3

- Tên dự toán mua sắm: Kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin mức độ 3

- Chủ đầu tư: Trung tâm Giám Sát Điều Hành Đô Thị Thông Minh tỉnh Đắk Lắk.

- Địa điểm thực hiện: tỉnh Đắk Lắk.

- Nguồn vốn: Ngân sách tỉnh năm 2025.

- Thời gian thực hiện gói thầu: 45 ngày.

- Hình thức và phương thức lựa chọn nhà thầu: Chào hàng cạnh tranh trong nước, theo phương thức một giai đoạn, một túi hồ sơ, đấu thầu qua mạng.

- Loại hợp đồng: Trọn gói.

- Quy mô thực hiện

+ Kiểm tra, đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh Đắk Lắk

+ Kiểm tra, đánh giá an toàn thông tin cho ứng dụng đang sử dụng.

- **Yêu cầu về cung cấp dịch vụ:**

➢ **Yêu cầu chung:** Đối với từng đối tượng đánh giá cần tuân theo (bao gồm nhưng không giới hạn) các hướng dẫn, tiêu chuẩn theo danh sách dưới đây:

+ Đối với hạ tầng công nghệ thông tin sử dụng kết hợp Technical Guide to Information Security Testing and Assessment của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST) và Open Sources Security Testing Methodology Manual (OSSTMM).

+ Đối với các ứng dụng web/mobile tuân theo các hướng dẫn của OWASP cho việc kiểm thử xâm nhập, bao gồm OWASP Top 10 Web Application Security Risks, OWASP Top 10 Mobile Risks, OWASP Top 10 API Security.

➢ **Yêu cầu về kiểm tra, đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh Đắk Lắk:**

+ Sử dụng kết hợp Technical Guide to Information Security Testing and Assessment (SP 800-115) của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST) và Open

Source Security Testing Methodology Manual (OSSTMM) cho việc kiểm soát đánh giá điểm yếu các thành trong hệ thống như máy chủ, thiết bị mạng.

➢ **Yêu cầu kiểm tra, đánh giá an toàn thông tin cho ứng dụng đang sử dụng.**

- **Yêu cầu về kiểm tra, đánh giá an toàn thông tin cho Hệ thống Thư điện tử tỉnh Đắk Lắk**

+ Sử dụng kết hợp Technical Guide to Information Security Testing and Assessment (SP 800-115) của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST), Open Source Security Testing Methodology Manual (OSSTMM) và Open Web Application Security Project (OWASP) Testing Guide v4 cho việc kiểm soát đánh giá nhược điểm và thử nghiệm tấn công ứng dụng Thư điện tử để lấy bằng chứng.

Các kỹ sư bảo mật đóng vai trò như người tấn công, từ bên ngoài thực hiện kiểm thử toàn bộ các lỗi tìm ra, tiến hành các thao tác trái phép nhằm phát hiện các xử lý bất thường của hệ thống. Việc kiểm thử sẽ được thực hiện trong hai trường hợp: không có tài khoản và có tài khoản đăng nhập.

- **Yêu cầu về kiểm tra, đánh giá an toàn thông tin cho Hệ thống Quản lý văn bản và Điều hành tỉnh Đắk Lắk**.

+ Sử dụng kết hợp Technical Guide to Information Security Testing and Assessment (SP 800-115) của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST), Open Source Security Testing Methodology Manual (OSSTMM) và Open Web Application Security Project (OWASP) Testing Guide v4 cho việc kiểm soát đánh giá nhược điểm và thử nghiệm tấn công ứng dụng quản lý văn bản và điều hành để lấy bằng chứng.

Các kỹ sư bảo mật đóng vai trò như người tấn công, từ bên ngoài thực hiện kiểm thử toàn bộ các lỗi tìm ra, tiến hành các thao tác trái phép nhằm phát hiện các xử lý bất thường của hệ thống. Việc kiểm thử sẽ được thực hiện trong hai trường hợp: không có tài khoản và có tài khoản đăng nhập.

- Yêu cầu về kiểm tra, đánh giá an toàn thông tin cho Hệ thống Cổng thông tin điện tử tỉnh.

Sử dụng kết hợp Technical Guide to Information Security Testing and Assessment (SP 800-115) của Viện tiêu chuẩn và công nghệ Hoa Kỳ (NIST), Open Source Security Testing Methodology Manual (OSSTMM) và Open Web Application Security Project (OWASP) Testing Guide v4 cho việc kiểm soát đánh giá nhược điểm và thử nghiệm tấn công Cổng thông tin điện tử tỉnh để lấy bằng chứng.

Các kỹ sư bảo mật đóng vai trò như người tấn công, từ bên ngoài thực hiện kiểm thử toàn bộ các lỗi tìm ra, tiến hành các thao tác trái phép nhằm phát hiện các

xử lý bất thường của hệ thống. Việc kiểm thử sẽ được thực hiện trong hai trường hợp: không có tài khoản và có tài khoản đăng nhập.

2. Mục tiêu công việc:

Thuê đơn vị thực hiện kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin mức độ 3 đạt được các mục tiêu:

- Phát hiện lỗ hổng cấu hình và điểm yếu bảo mật qua đó ngăn chặn nguy cơ bị tấn công do lỗi vận hành hoặc sai sót con người.

- Đảm bảo hệ thống và thiết bị hoạt động đúng theo chính sách an ninh giảm thiểu các rủi ro và tăng cường kiểm soát.

- Tăng cường độ tin cậy cho hệ thống thông tin. Bảo vệ dữ liệu, duy trì hoạt động ổn định.

2.1 Nội dung khối lượng công việc:

- Kiểm tra, đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh Đắk Lắk gồm:

+ Thiết bị mạng (Switch, Router) và thiết bị bảo mật (Firewall, Web Application Firewall, Intrusion Detection System/Intrusion Prevention System, Load Balancer): 25 thiết bị

+ Máy chủ vật lý và máy chủ áo hoá; Hệ thống lưu trữ: 144 thiết bị

- Kiểm tra, đánh giá an toàn thông tin cho ứng dụng (gồm 3 hệ thống) gồm:

+ Hệ thống Thư điện tử công vụ tỉnh

+ Hệ thống Phần mềm Quản lý văn bản và điều hành (iDesk)

+ Hệ thống Cổng thông tin điện tử tỉnh

2.2 Chi tiết khối lượng công việc:

2.2.1. Kiểm tra, đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh Đắk Lắk

Phần 1: Hệ thống thiết bị mạng và bảo mật

STT	Tên thiết bị / phần mềm	Số lượng	ĐVT
I	**Thiết bị mạng (Switch, Router)**		Thiết bị
1	Thiết bị chuyển mạch lõi – Dell Switch S5048F	2	Thiết bị
2	Thiết bị chuyển mạch lõi – Dell Switch S3148	2	Thiết bị
3	Thiết bị chuyển mạch vùng Hosting – Dell Switch S3124	2	Thiết bị
4	Thiết bị chuyển mạch lõi – Cisco 9200L	2	Thiết bị
5	Thiết bị chuyển mạch SAN – SAN Switch Brocade 300	2	Thiết bị

II	**Thiết bị bảo mật (Firewall, Web Application Firewall, Intrusion Detection System/Intrusion Prevention System, Load Balancer)**		Thiết bị
1	Thiết bị tường lửa – Sophos XG210	2	Thiết bị
2	Thiết bị cân bằng tải ứng dụng – Citrix ADC MPX 5901	2	Thiết bị
3	Thiết bị tường lửa lớp biên – Palo Alto Networks PA-3220	2	Thiết bị
4	Thiết bị tường lửa lớp lõi – FortiGate 600E	2	Thiết bị
3	Thiết bị tường lửa mạng nội bộ – Sophos XG310	2	Thiết bị
5	Thiết bị tường lửa Hosting – Sophos XG210	2	Thiết bị
6	Thiết bị tường lửa bảo mật ứng dụng Web – Barracuda WAF 460	2	Thiết bị
7	Thiết bị tường lửa – Email Security Gateway Barracuda 400	1	Thiết bị

Phần 2: Hệ thống máy chủ vật lý, máy chủ ảo và hệ thống lưu trữ

STT	**Tên thiết bị / phần mềm**	**Số lượng**	ĐVT
III	**Máy chủ vật lý**		Thiết bị
1	Máy chủ Dell R730	11	Thiết bị
2	Máy chủ Dell R740	4	Thiết bị
IV	**Hệ thống lưu trữ**		Thiết bị
1	Thiết bị lưu trữ tập trung SAN IBM Flash System V5100	2	Thiết bị
2	Thiết bị lưu trữ tập trung – HPE MSA 2050	2	Thiết bị
3	Thiết bị lưu trữ tập trung – HPE MSA 2052	1	Thiết bị
4	Thiết bị lưu trữ tập trung – HPE MSA 2052 (Disk Shelf)	1	Thiết bị
5	Thiết bị lưu trữ tập trung – NAS HP Store Easy 1650	1	Thiết bị
6	Thiết bị lưu trữ băng từ – TAPE HP Store Ever MSL 2024	1	Thiết bị

Danh mục các máy chủ ảo hoá bao gồm:

Stt	**Tên máy chủ**
1	0_10.200_tftp.server.2020
2	01_02_TSLCD2-DNS_1.138
3	03-05-qlvb-LDAP-01_1.191
4	03-05-qlvb-LDAP-02_1.192
5	04-qlvb-tdnv-App_1.159
6	04-qlvb-tdnv-DB_2.159
7	1.110-Webapp-Daklak
8	1.114-TextToSpeech

9	1.lienthong_1.100_LT-VPCP
10	1.lienthong_1.101_LT-DVC
11	10_1.123_CT14-BKAV
12	11_1.121_VIENTHONGTHUDONG_BCVT
13	115_Kho_CSDL_01
14	116_Kho_CSDL_02
15	12_1.30-CBCCVC
16	2.100-Backup Dak Lak
17	2.112-Portal-Daklak
18	2.mail_1.70_mail01-70_CLONE
19	2.mail_1.72_webmail01-dla-72
20	2.mail_1.78_ldap02-78
21	2.qlvb_1.197_CAS
22	2.qlvb_1.198_all_domain
23	2.qlvb_1.199_all_domain
24	2.qlvb_1.22_LOTUS
25	2.qlvb_1.25_ESB_app
26	2.qlvb_1.26_ESB-truclienthong
27	2.qlvb_1.27_esb-backup
28	2.qlvb_1.29_SUM_DATABASE_Calendar
29	2.qlvb_1.38_Fileserver - 38
30	2022_QLVB-App-01_1.61
31	2022_QLVB-App-02_1.62
32	2022_QLVB-App-03_1.63
33	2022_QLVB-App-04_1.64
34	2022_QLVB-App-05_1.65
35	2022_QLVB-App-06_1.66
36	2022_QLVB-App-07_1.67
37	2022_QLVB-App-08_1.68
38	2022_QLVB-App-09_1.69
39	2022_QLVB-App-10_1.74
40	2022_QLVB-App-Daotao_1.71
41	2022_QLVB-App-DL-STC_1.31
42	2022_QLVB-App-KVB_1.21
43	2022_QLVB-DataNode-01_2.61
44	2022_QLVB-DataNode-02_2.62
45	2022_QLVB-DataNode-03_2.63
46	2022_QLVB-DataNode-04_2.64
47	2022_QLVB-DataNode-05_2.65

48	2022_QLVB-DataNode-06_2.66
49	2022_QLVB-DataNode-07_2.67
50	2022_QLVB-DB-01_2.71
51	2022_QLVB-DB-02_2.72
52	2022_QLVB-DB-03_2.73
53	2022_QLVB-DB-04_2.74
54	2022_QLVB-DB-05_2.75_KVB
55	2022_QLVB-DB-06_2.76
56	2022_QLVB-DB-07_2.77
57	2022_QLVB-DB-08_2.78
58	2022_QLVB-DB-09_2.79
59	2022_QLVB-DB-10_2.80_daotao
60	2022_QLVB-DBmysql_2.231
61	2022_QLVB-DBmysql_2.232
62	2022_QLVB-DBmysql_2.233
63	2022_QLVB-DBmysql_2.234
64	2022_QLVB-DBmysql_2.235
65	2022_QLVB-DBmysql_2.236
66	2022_QLVB-NameNode-01_2.70
67	2024_11_hoptructuyen_1-33
68	3.114-Database-DakLak
69	6-1.133_lgsp_IS
70	6-2.131_lgsp_LGSP01
71	6-2.132_lgsp_LGSP02
72	6-2.135_lgsp_Database
73	7.csdldc_1.80_WEB
74	7.csdldc_1.81_LDAP
75	7.csdldc_1.82_CSDL.LGSP02
76	7.csdldc_1.83_CSDL.APP01
77	7.csdldc_1.84_CSDL.APP02
78	7.csdldc_1.85_CSDL.DATABASES
79	7.csdldc_1.86_CSDL.DATABASES02
80	7.csdldc_1.87_DASHBOARD
81	8.NQ03DLA_1.93_DTDL App 01
82	8.NQ03DLA_1.94_DTDL App 02
83	8.NQ03DLA_1.95_DTDL DATABASES
84	8.NQ03DLA_1.96_DTDL LOADBLANCE
85	IOC-Web-SVR
86	NMS_SLCD_VNPT

87	PT_Manager_Temp
88	SPP-10.1.11-3010
89	SRV-DNS01
90	SRV-DNS02
91	SRV-Logcentalization
92	SRV-McAfee
93	SRV-NMS
94	SRV-ServiceDeskPlus
95	VMware vCenter Server - v7
96	VSNAP-10.1.11-72
97	14-webserver14
98	15-Webserver1Clonefrom20_2.15
99	17-webSLD_CloneFrom20
100	18-webserver18
101	2023_Camera_Valley_121
102	2023_Camera_VMS_122
103	20-WEBSITE-TX.BUONHO
104	23-webserver23
105	24-NQ42CP
106	32-BACKUP-HOSTING
107	42-hosting-backup
108	44-QuanLyThanhTra
109	54_WebServer-54
110	61_STC_CSDL_Gia_WEBSVR
111	62_STC_CSDL_Gia_DBSVR
112	Hosting - vCenter Server
113	IOC-Web-SVR
114	SOC_NSM-Sensor_7.5_LAN
115	SOC_Poller_7.7
116	SOC-NSM-Manager_7.6
117	SOC-SOAR_7.4
118	SRV-cPanel
119	SRV-Nginx01
120	SRV-Nginx02
121	WEBSERVER36

2.2.2. Các hệ thống phần mềm ứng dụng

- Hệ thống Thư điện tử công vụ tỉnh: 01 hệ thống
- Hệ thống Phần mềm Quản lý văn bản và điều hành (iDesk): 01 hệ thống

- Hệ thống Cổng thông tin điện tử tỉnh: 01 hệ thống

3. Yêu cầu kỹ thuật của gói thầu:

3.1. Nội dung công việc kiểm tra, đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh Đắk Lắk

- Nhà thầu trình bày chi tiết các công việc cho từng phần riêng biệt đảm bảo các hệ thống đều đảm bảo các hệ thống đều đạt được yêu cầu đầu ra.

Nội dung công việc	Yêu cầu về đầu ra
1. Khảo sát mục tiêu và thu thập thông tin	
- Xác định các kiểm soát truy cập và các yêu cầu an toàn thông tin của mỗi đối tượng, hệ thống. - Xác định xem đối tượng, hệ thống có chứa các dữ liệu nhạy cảm hay không, và cách thức dữ liệu nhạy cảm được trao đổi. - Ghi lại các thông tin về cấu hình cơ bản của các dịch vụ, các tiến trình, và các cổng mở trên các đối tượng, hệ thống. - Xác định các thiết bị trong phạm vi đánh giá: tên, địa chỉ IP, chủ sở hữu, … + Địa chỉ IP + Địa chỉ MAC + Tên thiết bị + Hãng sản xuất + Dòng thiết bị (Model, Name, Family) - Xác định, phân loại các nền tảng hệ điều hành của các thiết bị trong phạm vi đánh giá: Thông tin về hệ điều hành/firmware đang sử dụng. - Xác định tất cả các dịch vụ trên các thiết bị trong phạm vi đánh giá: Thông tin về số hiệu các cổng dịch vụ đang mở.	**Hồ sơ thông tin hệ thống:** Bao gồm sơ đồ mạng chi tiết, danh sách thiết bị kèm thông tin phiên bản firmware/HĐH, và danh sách các cổng dịch vụ đang mở.
2. Lập kế hoạch rà quét	
Lập kế hoạch rà quét chi tiết theo các thành phần được khảo sát trong phạm vi công việc thực hiện đánh giá bảo mật	Bản kế hoạch các công việc thực hiện rà quét chi tiết cho từng đối tượng.
3. Rà soát lỗ hổng:	
Thực hiện rà quét, kiểm tra và phát hiện các lỗ hổng, điểm yếu và các nguy cơ đang tồn tại, bao gồm: - Các lỗ hổng liên quan đến cơ chế xác thực (sử dụng tài khoản mặc định, sử dụng mật khẩu yếu, phổ biến, sử dụng tính năng xác thực yếu, kém an toàn).	**Báo cáo kết quả rà soát** gồm vị trí lỗ hổng, điểm yếu và thông tin đầy đủ liên quan đến các lỗ hổng, điểm yếu.

- Các lỗ hổng liên quan đến hệ điều hành thiết bị và các ứng dụng được cài trên thiết bị bao gồm các lỗ hổng do thiếu bản vá bảo mật. - Các lỗ hổng do lỗi cấu hình, triển khai cài đặt. - Kiểm tra các bản patch, update có được cài đặt đầy đủ - Dò quét điểm yếu trên các cổng dịch vụ đang chạy - Các lỗ hổng CVEs đã công bố	
4. Xác minh lỗ hổng	
- Tiến hành phân tích thông tin, đánh giá rủi ro, khả năng tấn công đối với các lỗ hổng, điểm yếu	Danh sách các lỗ hổng hoặc điểm yếu phát hiện được
5. Đánh giá mức độ nguy hiểm các lỗ hổng	
Thực hiện phân loại mức độ nguy hiểm của các lỗ hổng tìm được theo thang điểm Common Vulnerability Scoring System (CVSS 3.1) của National Institute of Standards and Technology (NIST)	**Báo cáo phân tích kỹ thuật:** Ghi lại chi tiết kết quả đánh giá từng hạng mục (cấu hình lớp 1/2/3, logging, xác thực, chính sách...). Liệt kê các lỗ hổng, điểm yếu, cấu hình sai được phát hiện, kèm theo bằng chứng và phân loại mức độ rủi ro.
6. Báo cáo và khuyến nghị	
Báo cáo kết quả đánh giá và hướng dẫn	**Báo cáo tổng hợp kết quả đánh giá (chính thức):** Bao gồm bản tóm tắt dành cho quản lý, mô tả các phát hiện chính, đánh giá mức độ ảnh hưởng và đưa ra các khuyến nghị khắc phục cụ thể, khả thi theo thứ tự ưu tiên.
7. Hướng dẫn người dùng thực hiện khắc phục các lỗ hổng theo khuyến nghị đã đưa ra.	
Hướng dẫn người dùng thực hiện khắc phục các lỗ hổng theo khuyến nghị đã đưa ra.	Tài liệu hướng dẫn người dùng thực hiện khắc phục các lỗ hổng theo khuyến nghị đã đưa ra.
8. Tái đánh giá sau khi khắc phục	
Tái đánh giá sau khi khắc phục	**Báo cáo kết quả tái đánh giá:** Xác nhận các lỗ hổng đã được khắc phục thành công, ghi nhận trạng thái an toàn mới của hệ thống và liệt kê các vấn đề còn tồn đọng (nếu có).

3.2. Nội dung công việc kiểm tra, đánh giá an toàn thông tin cho ứng dụng

- Nhà thầu trình bày chi tiết các công việc cho từng hệ thống phần mềm ứng dụng riêng biệt đảm bảo các hệ thống đều đảm bảo đảm bảo các hệ thống đều đạt được yêu cầu đầu ra.

Nội dung công việc	Yêu cầu về đầu ra
1. Khảo sát mục tiêu và thu thập thông tin	
- Thông tin về nghiệp vụ, chức năng ứng dụng; - Thông tin công nghệ, ngôn ngữ lập trình, nền tảng sử dụng, …; - Thông tin về domain, chứng chỉ SSL, địa chỉ IP Public, … liên quan đến ứng dụng; - Thông tin về các ứng dụng Web như địa chỉ IP máy chủ ứng dụng Web, vùng mạng đặt máy chủ ứng dụng Web, phiên bản và giải pháp sử dụng trên máy chủ ứng dụng Web; - Thông tin về các cơ sở dữ liệu mà ứng dụng Web đang sử dụng như giải pháp sử dụng, phiên bản, mục đích sử dụng, địa điểm cài đặt, ... - Thông tin về các giải pháp bảo mật đang được sử dụng cho ứng dụng web, … - Thông tin về các quy trình nghiệp vụ liên quan đến phía khách hàng khi truy cập ứng dụng, … - Phiên bản hiện hành cũng như thông tin liên quan đến máy chủ xử lý những yêu cầu từ ứng dụng… - Xác định cấu trúc, chức năng của ứng dụng, lên sơ đồ hoạt động…	**Hồ sơ thông tin hệ thống:** Bao gồm các nghiệp vụ, chức năng,nền tảng, ngôn ngữ … các thông tin liên quan đến từng ứng dụng
2. Lập kế hoạch rà quét	
Lập kế hoạch rà quét chi tiết theo các thành phần được khảo sát trong phạm vi công việc thực hiện đánh giá bảo mật	Bản kế hoạch các công việc thực hiện rà quét chi tiết cho từng ứng dụng
3. Rà soát lỗ hổng:	
- Kiểm tra về thu thập thông tin (Information Gathering). - Kiểm tra về quản lý cấu hình và triển khai (Configuration and Deployment Management Testing). - Kiểm tra về quản lý định danh (Identity Management Testing).	**Hồ sơ thông tin hệ thống:** Tài liệu chi tiết ghi lại kết quả của từng hạng mục kiểm tra.

- Kiểm tra về xác thực (Authentication Testing). - Kiểm tra về phân quyền (Authorization Testing). - Kiểm tra về quản lý phiên làm việc (Session Management Testing). - Kiểm tra về tính hợp lệ của dữ liệu đầu vào (Input Validation Testing). - Kiểm tra về quản lý và xử lý lỗi (Error Handling). - Kiểm tra về thuật toán, giao thức mã hóa yếu (Cryptography). - Kiểm tra về chức năng nghiệp vụ (Business Logic Testing). - Kiểm tra về dữ liệu đầu ra phía người dùng (Client Side Testing).	
4. Xác minh lỗ hổng và tấn công kiểm thử	
- Kiểm tra lỗ hổng A01:2021-Broken Access Control; - Kiểm tra lỗ hổng A02:2021-Cryptographic Failures; - Kiểm tra lỗ hổng A03:2021-Injection; - Kiểm tra lỗ hổng A04:2021-Insecure Design - Kiểm tra lỗ hổng A05:2021-Security Misconfiguration - Kiểm tra lỗ hổng A06:2021-Vulnerable and Outdated Components - Kiểm tra lỗ hổng A07:2021-Identification and Authentication Failures - Kiểm tra lỗ hổng A08:2021-Software and Data Integrity Failures; - Kiểm tra lỗ hổng A09:2021-Security Logging and Monitoring Failures; - Kiểm tra lỗ hổng A10:2021-Server-Side Request Forgery	Danh sách các lỗ hổng hoặc điểm yếu: bao gồm danh sách các lỗ hổng, điểm yếu cấu hình được phát hiện, kèm theo bằng chứng kỹ thuật (VD: ảnh chụp màn hình, mã khai thác) và kịch bản tấn công thử
5. Đánh giá mức độ nguy hiểm các lỗ hổng	
Thực hiện phân loại mức độ nguy hiểm của các lỗ hổng tìm được theo thang điểm Common Vulnerability Scoring System (CVSS 3.1) của National Institute of Standards and Technology (NIST)	**Báo cáo phân tích kỹ thuật:** phân loại mức độ rủi ro (Cao, Trung bình, Thấp).
6. Báo cáo và khuyến nghị	

Báo cáo đánh giá phát hiện các về các lỗ hổng theo các mức độ nguy hiểm, kèm theo đó là hình ảnh minh họa cách thức, kết quả quá trình đánh giá, đề xuất các phương án, giải pháp để khắc phục các lỗ hổng, điểm yếu bảo mật được phát hiện	**Báo cáo tổng hợp kết quả đánh giá (chính thức):** **Chi tiết phát hiện:** Mô tả từng lỗ hổng, mức độ rủi ro, kết quả tấn công thử hệ thống. - **Khuyến nghị khắc phục:** Các hướng khuyến nghị, đề xuất để khắc phục
7. Hướng dẫn người dùng thực hiện khắc phục các lỗ hổng theo khuyến nghị đã đưa ra.	
Hướng dẫn người dùng thực hiện khắc phục các lỗ hổng theo khuyến nghị đã đưa ra.	Tài liệu hướng dẫn chi tiết các bước sửa lỗi, nâng cấp, hoặc thay đổi cấu hình theo thứ tự ưu tiên.
8. Tái đánh giá sau khi khắc phục	
Tái đánh giá sau khi khắc phục	**Báo cáo kết quả tái đánh giá:** Xác nhận các lỗ hổng đã được khắc phục thành công, ghi nhận trạng thái an toàn mới của hệ thống và liệt kê các vấn đề còn tồn đọng (nếu có).

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.

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

+ Báo cáo tổng kết đánh giá điểm yếu an ninh cho các hạng mục (cho các lần đánh giá): 03 bản gốc

+ Biên bản nghiệm thu công việc cho các hạng mục dịch vụ: 03 bản gốc

+ Biên bản nghiệm thu hoàn thành dịch vụ: 03 bản gốc

+ Cam kết hỗ trợ kỹ thuật xử lý khi xảy ra các vấn đề mất ATTT đối với các hạng mục là 12 tháng: 03 bản gốc.