EMAGINED SECURITY

Penetration Test Project Management Questionnaire

CLIENT: _____

DATE: _____

The purpose of this document is to assist in planning and scoping the overall engagement.

1. What are the key reasons for performing a Penetration Test Risk Assessment?

2. What are you trying to achieve by performing this assessment?

3. List any other milestones/tasks you would like to see accomplished during the assessment.

4. Who are the key players involved in the assessment purchase process? (Names/Titles/Phone/Email please)

5. Who has authorization to sign off on the project?

6. What are the steps that need to be completed should you decide to procure Emagined Security's consulting services?

7. What is your estimated timeline for making a final decision?

8. Do you have a preferred tentative start date?

9. How long does it take to provision access for consultants (for example, account access if required, badges, space)?

10. When does your project need to be completed? What are your internal deadlines?

EMAGINED SECURITY

Penetration Test Project Scoping Questionnaire

CLIENT: _____

DATE: _____

The purpose of this document is to assist in scoping audit engagements within complex information technology environments. You only need to fill out parts that are in scope of your assessment requirements.

Part I – External Network Penetration Testing

Please identify the amounts for the following that will be considering in the scope of the review:

	Number
Total number of external IPs within the address range owned and/or operated by your company:	_____
Maximum Number of Active IPs:	_____

Will active countermeasures be in place during testing?

Can testing source IP's be white-listed from active countermeasures (shunning)?

Are any third parties (service providers) in scope? (e.g., Azure, AWS, Remote Data Center)

Please indicate what level test you are currently anticipating / require (see attachment for level descriptions):

- Level 0 – Vulnerability Scan ☐
- Level 1 – Vulnerability Assessment ☐
- Level 2 – Defined Penetration Test (Typical Level) ☐
- Level 3 – Enhanced Penetration Test (Red Team) ☐

Part II – Internal Network Penetration Testing

Please identify the amounts for the following that will be considering in the scope of the review:

	Number
Number of network subnets (class C) to be scanned:	_____
Total Number of Active IPs:	_____
Can all IP addresses be accessed from one location/assigned IP address? If not, how many physical locations will testing be required:	_____

Are any third parties (service providers) in scope? (e.g., Azure, AWS, Remote Data Center)

Is PCI DSS Segmentation Testing Required? (e.g., CDE)

Please indicate what level test you are currently anticipating / require (see attachment for level descriptions):

- Level 0 – Vulnerability Scan ☐
- Level 1 – Vulnerability Assessment ☐
- Level 2 – Defined Penetration Test (Typical Level) ☐
- Level 3 – Enhanced Penetration Test (Red Team) ☐

Part III – Application Penetration Testing (Per Application)

What is the purpose of the application?

What is the total page count?

	Yes	No
Will testing be available from the Internet?	☐	☐
Is authenticated testing included in the scope?	☐	☐
If Yes, a demo of the site will be requested		
Does it store PHI, PII or other sensitive data?	☐	☐
Is there a Web application firewall (WAF) in place?	☐	☐
Are APIs/AJAX/Service calls being used and need to be tested? If so, how many?	☐	☐
Is a Code review of the application desired?	☐	☐
What language(s) is it written in (e.g. .php, java, .Net, etc…)?		
What language is the backend database?		
Are any third parties (service providers) in scope? (e.g., Azure, AWS, Remote Data Center)	☐	☐

Please indicate what level test you are currently anticipating / require (see attachment for level descriptions):

- Level 0 – Vulnerability Scan ☐
- Level 1 – Vulnerability Assessment ☐
- Level 2 – Defined Penetration Test (**Typical Level**) ☐
- Level 3 – Enhanced Penetration Test (Red Team) ☐

TIER Limits

Tier	Number of Web Applications	Max Number of Editable Pages	Max Number of Input Fields	Max Authentication Method	Max Number of User Roles Tested	Includes Web Services Checks	Includes Server Network Configuration Checks	Includes Basic Level Database Checks
1	1	3	25	None	N/A	No	No	No
2	1	10	35	Simple: User / Password	2	Yes	No	Yes
3	1	20	50	Multi-Factor	5	Yes	Yes	Yes
4	1	40	75	Multi-Factor	5	Yes	Yes	Yes
5	1	60	100	Multi-Factor	5	Yes	Yes	Yes
6	Custom	Custom	Custom	Custom	Custom	Custom	Custom	Custom

Applications In Scope

Please select the Tier Level for the application that will be considering in the scope of the review:

Tier 1: Web Application (Simple Static Site) _____

Sample:
1 Website
1-3 Editable Pages
Configuration Checks of Servers Housing Web Applications
Database Information Stored
Database Information Referenced
Total Number of Input Fields for all Web Pages > 25
No Authentication
Use of Web Services

Tier 2: Web Application (Small Dynamic Site with Simple Administration) _____

Sample:
1 Website
4-10 Editable Pages
2 Roles
Configuration Checks of Servers Housing Web Applications
Database Information Stored
Database Information Referenced
Total Number of Input Fields for all Web Pages > 25
Basic Authentication
Use of Web Services

Tier 3: Web Application (Medium Dynamic Site with Complex Administration) _____

Sample:
1 Website
10-20 Editable Pages
2-5 Roles
Configuration Checks of Servers Housing Web Applications
Database Information Stored
Database Information Referenced
Total Number of Input Fields for all Web Pages > 25
Multiple Factors of Authentication (Token/Certificate/Biometric)
Use of Web Services

Tier 4: Web Application (Large Dynamic Site with Complex Administration) _____

Sample:
1 Website
20-40 Editable Pages
2+ Roles
Configuration Checks of Servers Housing Web Applications
Database Information Stored
Database Information Referenced
Total Number of Input Fields for all Web Pages > 25
Multiple Factors of Authentication (Token/Certificate/Biometric)
Use of Web Services

Tier 5: Web Application (Very Large Dynamic Site with Complex Administration) _____

Sample:
1 Website
40-60 Editable Pages
2+ Roles
Configuration Checks of Servers Housing Web Applications
Database Information Stored
Database Information Referenced
Total Number of Input Fields for all Web Pages > 25
Multiple Factors of Authentication (Token/Certificate/Biometric)
Use of Web Services

Tier 6: Web Application (Two or More Interlinked Sites) / Custom Application _____

Custom Applications will be based on individual requirements.
This is for tests that do not meet the above criteria

Sample:
2 Websites – User and Management Sites (Sites are related in usage)
15 - 20 pages to be fully analyzed for security vulnerabilities
2 - 6 Roles to be analyzed (e.g., 2 users, 2 supervisors, 1 super user, 1 administrator)
Database usage for authentication or data retention (including administrator role)
Application Access Control (e.g., functions restricted by user type)
Dedicated Administration Site
Credit Card numbers used or retained or Non Public Personally Identifiable information stored or retained in database

Part IV – Wireless Testing

Please identify the amounts for the following that will be considering in the scope of the review:

	Number
Number of Access Points:	_____
Number of SSID's in scope	_____
Number of Buildings:	_____

Please list the addresses that require wireless onsite testing:

1) _____

2) _____

3) _____

Attachment: Penetration Test Service Level Definitions

Level 0 – Vulnerability Scan:

The Emagined Security level zero "Vulnerability Scan" provides customers with a simple infrastructure and/or application scan using commercial and open source tools. This service provides an organization with the necessary information to begin securing their environment and may later be followed by another more thorough assessment.

This version includes a basic scan to satisfy regulatory requirements utilizing a single vulnerability tool. The associated deliverable is limited to only raw reports from the tool. No CONSULTANT analysis on results will be performed.

Level I – Vulnerability Assessment:

The Emagined Security level one "Vulnerability Assessment" consists of automated and manual scans of infrastructure and/or applications for security vulnerabilities. All automated scanning is augmented with manual verification of potential vulnerabilities. Minimal exploitation is performed at this level.

Reporting at this level is fully customized and consists of all discovered vulnerabilities.

Level II – Defined Penetration Test:

The Emagined Security level two "Defined Penetration Test" consists of automated and manual scans of infrastructure and/or applications for security vulnerabilities. This version includes the Vulnerability Assessment and adds exploitations of the vulnerabilities within the defined scope. All automated scanning is augmented with manual verification of potential vulnerabilities. This level of assessment includes manual testing for logical vulnerabilities in web applications and exploitation of select vulnerabilities (unsafe exploitation may take place at customer discretion).

This is a cooperative assessment to ensure coverage of defined target systems and applications.

Reporting at this level is fully customized and consists of all discovered and exploited vulnerabilities.

Level III – Expanded Penetration Test (Red Team):

The Emagined Security level three "Expanded Penetration Test" consists of automated and manual scans of infrastructure and/or applications for security vulnerabilities. This version includes the Defined Penetration Test and adds attempts to use the exploited vulnerabilities to compromise systems behind the initial targets. All automated scanning is augmented with manual verification of potential vulnerabilities. This level of assessment includes manual testing for logical vulnerabilities in web applications and exploitation of all potential vulnerabilities (unsafe exploitation may take place at customer discretion). During this process, exploitation takes place at all levels of the target environment.

- Additionally, Expanded Penetration Testing can be used to:
- Evaluate the organization's security awareness
- Validate the effectiveness of existing security controls
- Attempt to compromised and / or circumvent security control undetected
- Evaluate intrusion detection effectiveness
- Assess incident response identification and response effectiveness
- Test incident response capabilities

Reporting at this level is fully customized and consists of all discovered and exploited vulnerabilities.