

Pen Test Scoping Questionnaire

RDCTD | rdctd.com | c@rdctd.com

How to complete and return this form

- 1. Fill in the fields using Adobe Acrobat Reader, Chrome, Edge or Preview. Skip what does not apply.
- 2. Estimates are fine. Do not include passwords, keys or other credentials.
- 3. Save the completed PDF (File > Save, or Print > Save as PDF).
- 4. Email the saved PDF as an attachment to c@rdctd.com. Use the subject "Pen test scoping - your company name".

You can also complete the short version online at www.rdctd.com/pentest-questionnaire. Tell us what you would like tested and we will follow up with questions, so you only need the sections below that apply to your engagement.

About you

Legal business name	Company website
Primary contact (name and title)	Primary contact email
Primary contact phone	Billing (AP) contact email
Billing (AP) contact phone	Preferred billing currency
	Select...
Address	Industry
Number of employees	Estimated budget
	Select...
Preferred testing start date	Draft report needed by
Final report needed by	Preferred testing window
	Select...
Retest required after remediation?	Compliance requirements (SOC 2, PCI DSS, ISO 27001, HIPAA...)
Select...	

What would you like tested?

Tick everything that applies. Then complete the matching detail section further on.

Infrastructure

- | | |
|--|---|
| ☐ Infrastructure Penetration Test | ☐ Assumed-Breach Penetration Test |
| ☐ Attack Surface Penetration Test | ☐ Wireless Penetration Test |
| ☐ Vulnerability Assessment (quarterly or monthly) | ☐ Operational Technology (OT) Penetration Test |

Cloud

☐ Cloud Penetration Test

☐ Cloud Security Configuration Review (CIS Benchmark)

Is cloud testing required for compliance?

Select...

Applications

☐ Web Application Testing

☐ Mobile Application Testing

☐ AI / LLM Application Testing

☐ Thick Client Application Testing

Advanced

☐ Red Teaming

☐ Purple Teaming

☐ Social Engineering

☐ Security Maturity Assessment

☐ Physical Hardware Testing

Goals, timing, or anything else we should know

Application Security Testing

Complete if you selected web, mobile, AI or thick client testing.

Web applications

Web application 1

Application

URL

Purpose

Authentication

of dynamic pages

of API endpoints

of user roles

Single page app?

Select...

Custom-developed?

Serverless?

LLM / AI features?

If GraphQL: queries, mutations

Select...

Select...

Select...

Web application 2

Application

URL

Purpose

Authentication

of dynamic pages

of API endpoints

of user roles

Single page app?

Select...

Custom-developed? Select...	Serverless? Select...	LLM / AI features? Select...	If GraphQL: queries, mutations
---	---	--	--

Web application 3

Application 	URL
Purpose 	Authentication

# of dynamic pages 	# of API endpoints 	# of user roles 	Single page app? Select...
--	--	---	--

Custom-developed? Select...	Serverless? Select...	LLM / AI features? Select...	If GraphQL: queries, mutations
---	---	--	--

AI / LLM features (if applicable)

Based on an existing pre-trained model? Select...	How many LLMs are there to test?
What is the purpose of the LLM? 	How is it integrated (chatbot, summary, text generation...)?
Test the rest of the application, or only the LLM and its API? 	Custom integrations with other systems?
Trained or grounded on your own data? Sensitive information concerns? 	

Mobile applications

Mobile application 1

Application 	Cross-platform framework (React Native, Flutter...)
-------------------------------------	---

iOS? Select...	Android? Select...	Native (Kotlin/Swift)? Select...
--	--	--

Same APIs as web app? Select...	# of user roles 	# of API endpoints
---	---	--

Mobile application 2

Application 	Cross-platform framework (React Native, Flutter...)
-------------------------------------	---

iOS? Select...	Android? Select...	Native (Kotlin/Swift)? Select...
--	--	--

Same APIs as web app? Select...	# of user roles 	# of API endpoints
---	---	--

Thick client applications

Thick client application 1

Application

Platform

Code base

Serialized data?

of forms / screens

of user roles

of API endpoints

Thick client application 2

Application

Platform

Code base

Serialized data?

of forms / screens

of user roles

of API endpoints

Additional scoping notes

On-Prem Infrastructure Penetration Testing

Use a separate column for each location if your environment spans more than one site. Approximate figures are fine.

of external targets

Location 1

Location 2

Location 3

Location 4

of live external IPs

Location 1

Location 2

Location 3

Location 4

of internal targets

Location 1

Location 2

Location 3

Location 4

Identity provider

Location 1

Location 2

Location 3

Location 4

of physical servers

Location 1

Location 2

Location 3

Location 4

of VMs

Location 1

Location 2

Location 3

Location 4

of endpoints (end-user devices, workstations)

Location 1 	Location 2 	Location 3 	Location 4
Type of endpoints			
Location 1 Select...	Location 2 Select...	Location 3 Select...	Location 4 Select...
End-user work environment			
Location 1 Select...	Location 2 Select...	Location 3 Select...	Location 4 Select...
# of network components (firewalls, routers, switches, access points, load balancers)			
Location 1 	Location 2 	Location 3 	Location 4
# of Active Directory domains (on-prem and cloud combined)			
Location 1 	Location 2 	Location 3 	Location 4
EDR / XDR in use (e.g., SentinelOne, CrowdStrike)			
Location 1 	Location 2 	Location 3 	Location 4
Any OT assets in the in-scope IT environment?			
Location 1 Select...	Location 2 Select...	Location 3 Select...	Location 4 Select...
If yes, is OT segmented from IT?			
Location 1 Select...	Location 2 Select...	Location 3 Select...	Location 4 Select...
Where are your servers hosted?			
Location 1 Select...	Location 2 Select...	Location 3 Select...	Location 4 Select...
PCI segmentation testing required? Select...		If yes, how many CDEs (cardholder data environments)? 	
Wireless: how many SSIDs are in scope? 		Wireless: how many locations are in scope? 	
Attack surface: how many company domains are in scope? 		Active Directory configuration audit? Select...	
Active Directory password audit? Select...			
Additional scoping notes 			

Cloud Infrastructure Penetration Testing

Complete only the platforms you use.

Azure

Purpose (what do you use the cloud environment for?)

of tenants

of subscriptions

of resources across all resource groups

of VMs across all resource groups

Internal or external Kubernetes testing?

Select...

of Kubernetes clusters (AKS / ARO)

of pods / containers

of storage accounts

of Azure Functions / Runbooks / Logic Apps

AWS

Purpose (what do you use the cloud environment for?)

of AWS accounts in scope

of regions in scope

of virtual machines (EC2)

of storage buckets (S3)

of serverless functions (Lambda)

Internal or external Kubernetes testing?

Select...

of container clusters (EKS / ECS)

of pods / containers

of resources in Resource and Tag Editor

GCP

Purpose (what do you use the cloud environment for?)

of organizations in scope

of projects in scope

of regions in scope

of Compute Engine instances

of storage buckets

of serverless functions (Cloud Run)

Internal or external Kubernetes testing?

of Kubernetes clusters (GKE)

of pods / containers

of resources in Asset Inventory

Additional scoping notes

Assumed-Breach Penetration Testing

Is penetration testing required for compliance?

How many penetration tests do you perform annually?

Detection and monitoring handled by...

Preferred starting point (user laptop, VPN account, cloud user...)

Operational Technology (OT) Penetration Testing

of PLCs / critical infrastructure devices (high risk)

of misc. OT devices (medium risk)

of misc. OT devices (low risk)

of OT environments

Network diagram spanning IT and OT exists?

Asset list for OT, IT and external assets exists?

Contact info for both IT and OT staff?

Social Engineering

Tick the activities you would like included.

☐ Card cloning

☐ Device planting

☐ USB drops

☐ Phishing campaign

☐ MFA vishing campaign

☐ Tailgating

Red Teaming

How many users are in your environment?

How many cloud and on-prem environments?

Operational technology component?

Blue team

Include a purple team workshop add-on?

Select...

Number of objectives (reach finance systems, obtain domain admin...)

Starting points

☐ External contractor access

☐ Physical laptop

☐ Internal RDS or Citrix access

☐ Custom scenario

Purple Teaming

☐ Level 1: validate alerts, rules and logging gaps

☐ Level 2: attempt to bypass rules and defensive technology

Blue team

Select...

☐ Include external

☐ Include cloud

☐ Include collaborative attack validation support

☐ Include internal

☐ Include social engineering

Physical Hardware Testing

Willing to provide root and source code access?

Select...

Operating system and processor architecture

Debug interfaces exposed (UART, JTAG, SPI, I2C)?

Select...

Device name / model and number of units

Can devices be shipped to the testing team?

Select...

Firmware image available?

Select...

Security Maturity Assessment

Written incident response policy?

Select...

Written information security policies?

Select...

IT and security handled by the same people?

Select...

Develop software in-house?

Select...

Security procedures documented?

Select...

Legal or regulatory obligations (GDPR, PIPEDA, CCPA...)

All done? Save this PDF and email it to c@rdctd.com

Attach the saved file and use the subject "Pen test scoping - your company name".

We will follow up with any clarifying questions before matching you with a testing partner.