rethinQ
SOLUTIONS

Security Services

Protect Proactively. Not Just Reactively.

Client Intake Questionnaire

Question. Qualify. Quantify.

Instructions

Please complete this questionnaire as thoroughly as possible prior to your Discovery Session. Your responses help us understand your current landscape and tailor our assessment to your specific needs.

If a question does not apply, please write "N/A". If you are unsure, provide your best estimate — we will validate all data during our assessment phase.

Estimated completion time: 30–45 minutes

Building smarter, more resilient systems by aligning technology, people and strategy. Unleashing potential at every level.

CONFIDENTIAL

Section A: Organization Information

Organization Name:

Primary Contact: **Title / Role:**

Email: **Phone:**

Industry / Vertical: **Organization Size:**

Headquarters: **# Physical Locations:**

Annual Revenue: **Security Budget:**

Engagement Scope:

■ Cyber Only ■ Physical Only ■ Combined

Brief Description of Organization:

Section B: Current Security Posture

Security Team? (Y/N): **Security Team Size:**

CISO / CSO / Lead: **Reports To:**

Security Function:

■ Internal ■ Outsourced ■ Hybrid ■ No Formal Function

Existing Security Capabilities:

■ Risk Assessment ■ Vulnerability Mgmt ■ Penetration Testing

■ Incident Response ■ Security Monitoring / SOC ■ Compliance Mgmt

■ Awareness Training ■ Physical Access Control ■ Video Surveillance

■ Emergency Response ■ Executive Protection ■ Guard Services

Security incidents (past 24 months):

What prompted this engagement?

■ CYBER SECURITY — Digital Infrastructure

Network & Endpoint:

■ On-Prem Servers ■ Cloud (AWS/Azure/GCP) ■ Hybrid Cloud

■ Remote Workforce ■ BYOD Policy ■ MDM

■ VPN / Zero Trust ■ EDR ■ SIEM / Logging

Cloud Provider: _____ **# Endpoints (approx):** _____

Firewall Vendor: _____ **Last Vuln Scan:** _____

Patch Management:

■ Automated ■ Manual ■ Ad Hoc ■ None

Data & Communications:

■ Email Security ■ Encryption at Rest ■ Encryption in Transit

■ DLP ■ Secure File Share ■ Backup & Recovery

■ MFA ■ SSO ■ IAM

Email Platform: _____ **Collaboration Tools:** _____

How is sensitive data classified and protected?

■ CYBER SECURITY — Compliance & Governance

Compliance Frameworks:

■ SOC 2 ■ ISO 27001 ■ NIST CSF

■ PCI DSS ■ HIPAA ■ GDPR

■ PIPEDA ■ CIS Controls ■ FedRAMP

■ CMMC ■ Industry-Specific ■ None / Unsure

Compliance Status:

■ Certified ■ In Progress ■ Gap Analysis Needed ■ Not Started

Last External Audit: _____ **Open Findings:** _____

Security Policies?

■ Comprehensive ■ Partial ■ None

Compliance deadlines or regulatory pressures:

Incident Response & Continuity:

IR Plan:

■ Tested ■ Documented ■ Informal ■ None

BCP:

■ Tested ■ Documented ■ Informal ■ None

Last Tabletop Exercise: _____ **Last DR Test:** _____

Cyber Insurance?

■ Yes ■ No ■ Exploring

Current IR capabilities and known gaps:

■ PHYSICAL SECURITY — Facilities & Access

Facility Types:

■ Corporate Office ■ Warehouse / Distribution ■ Manufacturing
■ Retail / Storefront ■ Data Center ■ Healthcare
■ Educational Campus ■ Multi-Tenant ■ Remote / Field
■ Construction Site ■ Event Venue ■ Residential

 # Facilities: **Total Sq Ft:**

Operating Hours: **After-Hours Access:**

Access Control Systems:

■ Key Cards / Fobs ■ Biometric ■ PIN / Keypad
■ Traditional Keys ■ Mobile Credentials ■ Turnstiles / Mantraps
■ Intercom / Buzzer ■ Visitor Mgmt System ■ No Formal Control

AC Vendor: **System Age (Yrs):**

Credential Management:

■ Centralized ■ Departmental ■ Ad Hoc ■ Unknown

Access control vulnerabilities/concerns:

■ PHYSICAL SECURITY — Surveillance & Emergency

Surveillance & Monitoring:

■ CCTV / IP Cameras ■ Analog Cameras ■ Intrusion Alarm
■ Motion Sensors ■ Glass Break Sensors ■ Central Monitoring
■ On-Site Guards ■ Contract Guards ■ AI-Enabled Cameras
■ No Surveillance

 # Cameras (approx): **Camera Vendor:**

Video Retention: **Monitoring Hours:**

Known surveillance gaps or blind spots:

Emergency Preparedness:

Emergency Plan:

■ Tested ■ Documented ■ Informal ■ None

Evacuation Procedures:

■ Posted & Practiced ■ Posted Only ■ None

Last Emergency Drill: _____ **Drill Frequency:** _____

Emergency Readiness:

■ Fire Alarm ■ Sprinkler System ■ AED on Site

■ First Aid Kits ■ Emergency Lighting ■ Backup Power

■ Mass Notification ■ Safe Room / Shelter ■ Active Threat Protocol

■ Crisis Comm Plan

Workplace safety incidents/concerns (past 24 months):

Section G: Security Culture & Personnel

Awareness Training:

■ Formal Program ■ Annual / Ad Hoc ■ None

Phishing Simulation:

■ Active ■ Planned ■ None

Last Phishing Click Rate: _____ **Training Completion %:** _____

Background Checks:

■ All Employees ■ Select Roles ■ None

Violence Prevention:

■ Yes ■ Partial ■ No

Executive Protection:

■ Yes ■ Under Review ■ Not Required

Describe overall security culture:

Section H: Security Goals & Priorities

Top 3 Security Priorities (Next 12 Months):

What does success look like?

■ Cyber Security — Urgency Assessment

	1	2	3	4	5
Cyber Risk Assessment & Strategy	■	■	■	■	■
Network & Infrastructure Security	■	■	■	■	■
Data Protection & Privacy	■	■	■	■	■
Compliance & Regulatory Alignment	■	■	■	■	■
Incident Response & Business Continuity	■	■	■	■	■
Security Awareness & Culture	■	■	■	■	■

■ Physical Security — Urgency Assessment

	1	2	3	4	5
Physical Risk Assessment & Strategy	■	■	■	■	■
Access Control & Perimeter Security	■	■	■	■	■
Surveillance & Monitoring	■	■	■	■	■
Workplace Safety & Emergency Prep	■	■	■	■	■
Executive & Personnel Protection	■	■	■	■	■
Security Operations & Governance	■	■	■	■	■

Authorization & Sign-Off

By signing below, I confirm that the information provided is accurate to the best of my knowledge. I authorize rethinQ Solutions to use the information and access the platforms referenced in this document for the purposes of our engagement.

Signature: _____ **Date:** _____

Printed Name: _____ **Title:** _____