rethinQ

SOLUTIONS

Cyber Security Services Division

Protect Proactively. Not Just Reactively.

Client Onboarding & Consulting Framework

Question. Qualify. Quantify.

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

info@rethinq.ca | 1-855-rethinQ (738-4467) | rethinq.ca

CONFIDENTIAL

1. Who We Are

rethinQ Solutions is not a firm. We are not an agency. We are a curated collective of elite, independent contractors who assemble under the rethinQ banner when the problem demands it — and dissolve when the work is done. No permanent payroll. No overhead-driven recommendations. No standing army waiting for a war.

We serve clients facing challenges that don't fit neatly into the service catalogues of established vendors. Our value isn't just what we deliver — it's the vantage point we bring. A different perspective on complex problems. Creative, tailored, unconventional.

We aim to build with AI, democratize knowledge, and provide value-based solutions and services for our clients.

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

Our Four Service Pillars

GROWTH	TECHNOLOGY	SECURITY	PEOPLE
Revenue acceleration, pipeline generation, digital presence, vendor coordination	AI integration, cloud strategy, digital transformation, systems architecture	Cyber and physical risk, compliance, incident response, property profiling	Psychometric-informed talent, corporate therapy, leadership, culture design

We assess before we advise. We measure before we build.

A strategic alternative. An agile perspective. A precise instrument.

2. Your rethinQ Associate

A Trusted Advisor Who Works For You — Not The Vendors

Every rethinQ Associate is a hands-on strategist with real-world execution experience. They embed with your team, learn your business inside and out, and take full ownership of sourcing, negotiating, and overseeing every vendor relationship on your behalf — across cyber security and beyond. One advisor. Full oversight. No competing agendas.

The Challenge

Cybersecurity firms, compliance consultants, MSSPs, and insurance brokers are all pitching risk. Nobody is assessing your full digital exposure across infrastructure, data, compliance, and human factors — and nobody is coordinating the response.

The rethinQ Approach

Your rethinQ Associate evaluates your complete cyber risk posture across infrastructure, data, compliance, incident response, and security culture — then sources and manages the right partners across every dimension. One advisor for your entire cyber security strategy.

How It Works

1. Diagnose. Your Associate runs a comprehensive cyber security assessment to establish a clear baseline using rethinQ's proprietary intake questionnaires and maturity scorecards.

2. Source & Align. Instead of disconnected vendors, your Associate builds a unified cyber security strategy, sources the right specialists, and coordinates delivery across the full stack.

3. Measure & Sustain. Ongoing oversight with clear KPIs, sprint reviews, and quarterly reassessments. Your Associate holds every vendor accountable to measurable outcomes.

Built-in Accountability

One advisor. One cyber security strategy. One point of trust. Full vendor accountability. No more siloed agencies working at cross-purposes.

3. Cyber Security Services Division — Overview

The Cyber Security Services Division helps clients identify, assess, and mitigate risks to their digital assets, communications, and online footprint. We take a consultative, vendor-neutral approach — our recommendations are grounded in evidence and best practices, not tied to any specific product or platform.

From network architecture to endpoint protection, from compliance frameworks to incident response, our Cyber Security Division addresses the threats that exist in the digital landscape. Every engagement is anchored by a dedicated rethinQ Associate. For organizations seeking complete coverage, this division is designed to operate alongside our Physical Security Division as part of a unified security strategy.

Cyber Security Services Catalogue

Service Area	What We Deliver	Key Outcomes
Cyber Risk Assessment & Strategy	Threat landscape analysis, risk quantification, security posture evaluation, cyber risk register, executive risk reporting, security roadmap	Clear understanding of risk exposure, prioritized mitigation plan, board-ready reporting
Network & Infrastructure Security	Network architecture review, firewall and perimeter assessment, segmentation strategy, cloud security review, vulnerability scanning, pen testing coordination	Hardened perimeter, reduced attack surface, remediated vulnerabilities, secure cloud configurations
Data Protection & Privacy	Data classification, encryption strategy, DLP guidance, privacy impact assessments, data governance policies, cross-border data flow analysis	Protected sensitive data, regulatory compliance (PIPEDA, GDPR, HIPAA), reduced breach risk
Compliance & Regulatory Alignment	Gap analysis (SOC 2, ISO 27001, NIST CSF, PCI DSS, CIS Controls), audit prep, policy development, control mapping, evidence collection	Compliance readiness, reduced audit findings, documented control environment
Incident Response & Business Continuity	IR plan development, tabletop exercises, playbook creation, BCP, DR assessment, crisis communication frameworks	Tested response capabilities, reduced mean time to respond, organizational resilience
Security Awareness & Culture	Awareness program design, phishing simulations, executive briefings, security champion programs, human risk assessment	Reduced human-factor risk, security-conscious culture, measurable behaviour change

4. Client Onboarding Framework

Every Cyber Security engagement follows a structured five-phase onboarding process. Your rethinQ Associate guides you through each phase, ensuring deep understanding of your security posture, risk tolerance, and regulatory environment before recommending solutions. When clients also engage the Physical Security Division, the two onboarding tracks run in parallel with unified reporting.

Phase 1: Discovery & Intake (Week 1)

Objective: Understand the client's current cyber security posture, organizational context, threat landscape, and regulatory requirements.

Key Activities:

- Conduct a 90-minute Executive Discovery Session with senior leadership, IT/security leadership, and key stakeholders
- Distribute and collect the rethinQ Cyber Security Intake Questionnaire covering digital assets, infrastructure, compliance, IR readiness, and security culture
- Gather access to network diagrams, security policies, incident logs, vulnerability scan results, and compliance certifications
- Map the security decision-making structure and identify budget owners and operational stakeholders
- Conduct preliminary review of system architecture, cloud configuration, and identity management

Deliverable: Completed Cyber Security Profile & Discovery Summary Report

Phase 2: Current State Assessment (Weeks 2–3)

Objective: Perform a comprehensive audit across all cyber security functions to establish a maturity baseline and identify critical gaps.

Assessment Area	What We Evaluate	Scoring
Risk Management & Strategy	Cyber risk register, threat intelligence, risk quantification, executive reporting, security strategy alignment	1–5 Maturity Score (NIST CSF)
Network & Infrastructure	Architecture, segmentation, firewall config, cloud posture, vulnerability mgmt, endpoint protection, EDR/XDR	1–5 Maturity Score
Data Protection & Privacy	Data classification, encryption, DLP, privacy compliance, data governance, backup integrity	1–5 Maturity Score
Compliance & Controls	Framework alignment (SOC 2, ISO 27001, NIST, PCI), control effectiveness, audit readiness, third-party risk	1–5 Maturity Score
Incident Response & Resilience	IR plan testing, playbook maturity, communication protocols, MTTR, backup and recovery, BCP	1–5 Maturity Score

Assessment Area	What We Evaluate	Scoring
Security Culture & Awareness	Awareness program, phishing resilience, security champions, policy awareness, executive tone from the top	1–5 Maturity Score

Deliverable: rethinQ Cyber Security Maturity Scorecard — scored across all six dimensions with identified gaps and opportunities.

Phase 3: Gap Analysis & Service Matching (Week 4)

Objective: Translate assessment findings into a prioritized action plan, mapping gaps to specific rethinQ Cyber Security services and vendor partners.

Key Activities:

- Generate the Cyber Security Gap Matrix: current state vs. target state for each assessment dimension
- Prioritize gaps using a Risk-Impact framework (critical/immediate, high/short-term, medium/strategic, low/long-term), factoring threat likelihood, business impact, and regulatory exposure
- Match each gap to one or more rethinQ Cyber Security services with timelines, resource requirements, and dependencies
- Identify and shortlist vendor partners (MSSPs, pen testers, compliance auditors, EDR providers) — your Associate manages all sourcing and oversight
- Develop a phased Cyber Security Roadmap with milestones, quick wins, and long-term hardening initiatives
- Define KPIs and prepare preliminary investment estimates including insource vs. outsource recommendations

Service Matching Decision Logic

If Assessment Reveals...	Primary Service Match	Supporting Services
No risk register, ad hoc decisions, no executive reporting, misaligned spend	Cyber Risk Assessment & Strategy	Compliance & Regulatory, Security Culture
Unpatched systems, flat network, poor cloud config, weak endpoint protection	Network & Infrastructure Security	Risk Assessment, Incident Response
Unclassified data, weak encryption, no DLP, privacy gaps, poor backups	Data Protection & Privacy	Compliance & Regulatory, Network Security
Failed audits, no framework alignment, weak policy documentation	Compliance & Regulatory Alignment	Data Protection, Risk Assessment
No IR plan, untested backups, slow detection, no communication protocol	Incident Response & Business Continuity	Network Security, Risk Assessment

If Assessment Reveals...	Primary Service Match	Supporting Services
High phishing click rates, no awareness program, weak reporting culture	Security Awareness & Culture	Risk Assessment, Data Protection

Deliverable: Cyber Security Strategy Roadmap with prioritized recommendations, vendor shortlist, investment estimates, and projected outcomes.

Phase 4: Strategy Presentation & Alignment (Week 5)

Objective: Present findings and recommendations to leadership, align on priorities, and finalize engagement scope.

Key Activities:

- Deliver a formal Cyber Security Strategy Presentation with visual scorecards, risk heat maps, gap analysis, and the recommended roadmap
- Facilitate a collaborative risk prioritization workshop to align leadership on sequencing, acceptable risk thresholds, and budget allocation
- Refine engagement scope based on client feedback, budget constraints, internal capacity, regulatory timelines, and risk appetite
- Define the Statement of Work (SOW) including timelines, milestones, vendor assignments, governance structure, and escalation procedures
- Establish communication cadence (weekly stand-ups, bi-weekly sprint reviews, monthly executive security briefings, quarterly reviews)

Deliverable: Signed Statement of Work, finalized project plan, risk mitigation priorities, and assigned rethinQ Associate and security team.

Phase 5: Engagement Kickoff & Execution (Week 6+)

Objective: Transition from assessment into active execution with clear ownership, vendor oversight, sprint cycles, and iterative delivery.

Key Activities:

- Your rethinQ Associate assumes ownership of all vendor relationships and active service engagements
- Launch the first 30-day sprint with defined objectives, security controls to implement, and measurable targets
- Deploy security dashboards and KPI tracking tied to the Cyber Security Maturity Scorecard baseline
- Execute prioritized remediation: policy development, system hardening, control implementation, training deployment
- Conduct weekly operational stand-ups and bi-weekly sprint reviews with the client's security lead
- Deliver a 30-day Progress Report with security posture improvements, risk reduction metrics, and recommended adjustments

Deliverables: Active service delivery, security documentation, KPI dashboards, 30/60/90-day progress reports, quarterly security reviews.

5. Onboarding Timeline Summary

Timeline	Phase	Key Output	Client Commitment
Week 1	Discovery & Intake	Cyber Security Profile & Discovery Summary	4–6 hours + access provisioning
Weeks 2–3	Current State Assessment	Cyber Security Maturity Scorecard	System access + team availability
Week 4	Gap Analysis & Service Matching	Cyber Security Strategy Roadmap	2–3 hours
Week 5	Strategy Presentation & Alignment	Signed SOW & Project Plan	2–4 hours
Week 6+	Engagement Kickoff & Execution	Active Delivery + Dashboards	Ongoing weekly stand-ups

6. What Your rethinQ Associate Manages

From penetration testing to SOC 2 prep to incident response — your rethinQ Associate coordinates your full cyber security program. No more gaps between vendors. One strategy, one advisor, complete digital coverage.

- Managed Security Service Providers (MSSPs) and SOC vendors
- Penetration testing firms and red team engagements
- Compliance auditors and assessment firms (SOC 2, ISO, NIST)
- EDR/XDR vendors, SIEM platforms, and security tooling
- Cyber insurance brokers and incident response retainers
- Security awareness platforms and phishing simulation providers

7. Maturity Scorecard — Scoring Guide

Each assessment dimension is scored on a 1–5 maturity scale. This scoring guide ensures consistency across assessments and provides clear benchmarks for client communication.

Score	Maturity Level	Description
1	Ad Hoc	No formal cyber security strategy or documented processes. Activities are reactive and inconsistent. Significant unmanaged risk and missed opportunities.
2	Emerging	Basic activities exist but lack structure, consistency, or measurement. Some awareness of gaps but no clear plan to address them.
3	Defined	Formal processes exist and are documented. Core metrics are tracked. Strategy in place but execution is inconsistent or under-resourced.
4	Managed	Strategy is well-executed and data-driven. Processes are optimized with regular iteration. Performance meets or exceeds industry benchmarks.
5	Optimized	Industry-leading performance. Continuous innovation, advanced automation, and predictive capabilities. The function is a competitive differentiator.

8. Engagement Models

rethinQ Cyber Security services are available in flexible engagement models designed to fit each client's budget, timeline, and internal capacity. Every model includes an embedded rethinQ Associate as the single point of accountability.

Model	Best For	Structure	Duration
Diagnostic Only	Independent assessment before committing to execution — ideal for board reporting, M&A, or organizational health checks	Phases 1–3: Discovery, Assessment, and Gap Analysis with full Scorecard and Roadmap	4–5 weeks
Project-Based	Targeted engagements with defined scope and deliverables	Full onboarding (Phases 1–5) scoped to specific service areas with fixed deliverables	2–6 months
Retainer / Managed Services	Ongoing program management with continuous oversight, periodic reassessments, and strategic support	Full onboarding followed by recurring monthly services with dedicated rethinQ Associate	6–12 months (renewable)

Model	Best For	Structure	Duration
Fractional CISO	Senior leadership without the full-time commitment	Part-time executive placement (10–20 hrs/week) to own and drive strategy	6+ months

Ready to rethinQ your cyber security strategy?

Every great engagement begins with a structured conversation. Reach out to start your Discovery phase.

info@rethinq.ca | 1-855-rethinQ (738-4467) | rethinq.ca

Stay curious & rethinQ your potential.