Broker's Onboarding Guide to Coalition

Thank you for partnering with Tarmika and Coalition. We are excited to work with you! We've created this Onboarding Guide to assist you as you get to know Coalition, including documents, links, and resources to help get you started. If you have any questions you can reach out to the contacts listed on this page.

Table of Contents

Helpful contacts

Administrative Questions/Requests (Including Loss Runs, Binders & Endorsements): help@coalitioninc.com

BORs: bor@coalitioninc.com

Finance/Billing: CoalitionUS.AR@coalitioninc.com

Submissions: submissions@coalitioninc.com

Renewals: renewals@coalitioninc.com

Appetite Information

Coalition has a broad cyber appetite that includes organizations with up to $5B in revenue.

We are able to offer cyber limits up to $15M on Primary and $10M on Excess (More details on Excess).
**Exclusions and limitations apply. See policy as issued and disclaimers.*

Restricted classes of business:
Restricted classes of businesses include but are not limited to: Payment processors, Data aggregators, Adult entertainment, Casinos (any casino operation), Cannabis, and Managed Service Providers (outsourced data and IT service managers). Any additional questions about specific account appetite can be directed to our underwriting and BD team.

Submissions

There are easy ways to quote with Coalition, one of the fastest is logging into Tarmika platform. Tarmika's **"Access Quote"** bridges to Coalition's platform where you can find many resources including claims examples, case studies, coverage comparisons and other educational tools.

You may also send submissions via email:

- Cyber submissions: submissions@coalitioninc.com
- We accept competitor applications as well via email

Multiple domains: All email and website domains must be included at the time of submission for cyber quotes. If additional domains are found post-bind or included in the signature bundle, a scan will be conducted and terms are subject to change.

Ransomware Supplemental Application

There are two different ways a Ransomware Supplemental Application (RSA) can present itself to the broker. Both are reviewed by our underwriting team who will update the quote statuses accordingly and communicate with the broker.

RSA required prior to quoting

Coalition will not display a quote in this scenario. The renewal quote will have the status 'Under Review' until the RSA is received and reviewed by our underwriting team.

RSA as part of contingency

Quotes will be released contingent upon completion of the RSA.

Renewals

Any renewal inquiries | renewal applications, binders or renewal correspondence: please email renewals@coalitioninc.com

- The standard renewal process involves re-underwriting the policyholder risk based on updated information. We require an updated, signed updated renewal application to offer renewal terms.
- 90 days prior to expiration, Coalition will provide you with a pre-filled renewal application, RSA (if required), updated Coalition Risk Assessment, and updated loss runs.
- At least 30 days prior to renewal, an updated quote of insurance will be issued. If updated application information is not provided, a preliminary quote will be issued based on expiring information. These terms are subject to change based on any updated information received.

More information about Renewals at Coalition

Security Process

In order to establish an insurable baseline for each client, Coalition requires applicants to have essential protections in place before coverage can be bound. Brokers play a critical role as cyber advisors when preparing their clients to meet security requirements before they bind coverage. If applicants do not meet these requirements, a valid quote may be issued with specific conditions that must be satisfied before coverage can be bound. Coalition refers to these conditions as **contingencies**.

Types of technical contingencies

The most common types of technical contingencies are critical security findings and self-attestation security gaps.

Critical security findings

When applying for cyber insurance, we use cyber risk insights from our Active Data Graph to test the business' internet-exposed perimeter for exploitable security gaps. These are the same exposures threat actors are looking for in the wild and that our claims data shows as contributing to losses. If a serious exposure is detected, we flag it as a Critical Security Finding that often results in a contingency that must be resolved before binding. Brokers can learn more about some of our most common Critical Security Findings by accessing the explainer resources linked below:

- Remote Desktop Protocol (RDP): PDF | Video
- On-Premises MS Exchange: PDF | Video
- Exposed Risky Panels (Restrict Access): PDF | Video
- Exposed Risky Panels (MFA Required): PDF | Video

Self-attestation security gaps

Not all security exposures are visible and detectable by Coalition externally over the public internet. In order to get the full picture of a client's cyber risk profile we also rely on our cyber insurance application and/or Ransomware Supplemental Application (RSA). If a client's responses show critical security control gaps, we may require a client to implement additional controls before coverage can be bound.

Security & Contingency Resources

Broker Platform contingency view	Access detailed information about each technical contingency for new and renewal quotes. Download remediation resources to make it easier for clients to remediate and resolve technical contingencies. Learn more here.
Self-serve resources in Coalition Control	Clients can access technical details and remediation guidance for each critical security finding in their unique instance of Coalition Control. After the client remediates the exposure, the client can also access self-serve resources, trigger a rescan, and resolve each critical security finding with minimal broker involvement.
Pre-bind access to Coalition Control	Before your client even binds coverage, you can deliver access to the same security visibility and support clients will receive throughout the policy period. Pre-bind access also helps simplify contingency resolution by minimizing tasks for brokers and streamlining support for clients. Policyholders can also join a monthly onboarding webinar to familiarize themselves with Control.
Security support	Still have questions? For contingent new business quotes, schedule a call with a Coalition Security Engineer. For existing policyholders that need assistance resolving a midterm security alert email us at securitysupport@coalitioninc.com to work with a Security Support Specialist.
Managed Detection & Response (MDR)	To help strengthen your policyholders' security posture, Coalition offers Managed Detection and Response (MDR)[1] with potential premium discounts. More details on MDR

[1] Coalition Security Services MDR services are provided by Coalition Incident Response, Inc., an affiliate of Coalition

In-house Claims Process

Pre-claims assistance funds are included in every policy to allow policyholders to ask questions and seek guidance without fear of triggering a claim.

In the event of a suspected cyber incident, we recommend notifying our claims team as early as possible to limit the impact of a possible compromise. Our in-house claims team is available to assist 24/7 and will respond within an average of 5 minutes through email, phone or live chat.

EMAIL
claims@coalitioninc.com

PHONE
1 (833) 866-1337

LIVE CHAT
Available via our website

---

3 things to have on hand when reporting an incident:

1. Company information (company name and/or policy number)
2. Date of incident
3. Designated point of contact

Coalition Incident Response (CIR)

Policyholders can access the expertise of our affiliate, Coalition Incident Response (CIR)[2], for assistance with digital forensics and incident response upon discovery of a cyber incident. Learn more about policyholder benefits of working with CIR to quickly detect and stabilize a cyber event — often with no impact to their self-insured retention.

Additional helpful resources:

Details about our Panel Providers
Incident Preparedness Toolkits to guide policyholders on what to expect in the event of:

- Phishing
- Funds Transfer Fraud
- Ransomware

To access more resources and broker education tools, visit our Broker Resources page for more information.

[2] Coalition Incident Response (CIR) services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.