JENCAP®

Cyber Readiness Audit

MOVING BEYOND THE APPLICATION

Use this audit to assess whether a client's submission is ready for market or requires refinement before carrier review. Each checked box reflects a control that carriers consistently view as a strength. Gaps signal areas that may limit terms, trigger sublimits, or slow the placement, sometimes before the underwriter even raises a question.

1 IDENTITY & ACCESS: THE MFA FILTER

□ **Multi-Factor Authentication in Place**
Multi-factor authentication is enforced across all remote access points, including email and cloud-based applications, for all users.

□ **Privileged Accounts Secured**
Service and administrator accounts are protected using a password manager or privileged access tool, rather than shared credentials.

2 DATA RESILIENCY: THE RANSOMWARE FILTER

□ **Immutable or Air-Gapped Backups**
Backups cannot be altered or deleted by production systems and are isolated from the primary network.

□ **Restoration Tested**
Backup restoration speed and data integrity have been tested successfully within the last 90 days.

3 DETECTION & CONTAINMENT: THE VISIBILITY FILTER

□ **Continuous Endpoint Monitoring**
Endpoint detection and response tools are deployed across all devices and monitored 24/7 by a managed direct response (MDR) provider or security operations center (SOC).

□ **Network Segmentation Implemented**
Financial, employee, and other sensitive systems are isolated to limit lateral movement during an intrusion.

HOW TO EVALUATE THE AUDIT	**Rather than counting checkmarks, review what the gaps indicate about how the risk will be viewed once the submission reaches underwriting.**
All Boxes Checked	The submission reflects a strong cyber posture, so broader terms, competitive pricing, and manuscript enhancements are most achievable.
Gaps in Identity & Access	Access controls are a common trigger for decline. If remediation is feasible, address these items before the submission goes to market.
Gaps in Data Resiliency	Recovery concerns typically lead to ransomware sublimits or coinsurance. Carrier selection and breach-response support become more important here.
Gaps in Detection & Containment	These gaps suggest extended downtime risk. The submission should clearly document manual workarounds and continuity planning.

Translating Controls into Coverage Leverage

Now that you have your audit results, use them to shape the submission narrative. At this stage, technical controls become leverage to address coverage limitations that appear most often in cyber claims.

When the client has…	Watch for this gap…	So Jencap can help you…
Immutable Backups	Ransomware sublimits limiting recovery	**Challenge** restrictive sublimits and expand recovery protection
Segmented Networks	Low dependent business interruption (DBI) limits	**Align** DBI limits with full vendor outage exposure
24/7 Endpoint Detection and Response (EDR) Monitoring	Extended business interruption waiting periods	**Reduce** waiting periods based on response capability
Tested Incident Response Plan	Response costs eroding aggregate limits	**Structure** response expenses outside the primary limit

READY FOR A SUBMISSION REVIEW?

Waiting for the underwriter to identify gaps limits your options. But when you review the audit results early, you can adjust the submission to reflect the client's actual control environment and positions the placement for stronger terms. At Jencap, cyber specialists are often engaged at this stage to help translate security controls into coverage outcomes, supporting the work already being done and strengthening the placement before it's tested.

Your Jencap Cyber Specialist is ready and waiting.