This worksheet is not an application but outlines for brokers the basic information required in our AXIS Producer Portal to quote, bind, issue, or refer business for the respective coverage line. Additional information may also be required for certain risks or exposures. Please download the latest version from the AXIS Broker Resource Center. If you have any questions, please email AXISDigital@axiscapital.com.

Risk Assessment – Cyber Insurance

Protected Records

RECORD COUNT: Please provide an estimate of each type of record in your care, custody or control. (Note: One record represents a single individual regardless of the number of documents, transactions, or other data elements for that individual.)

What is your estimated total record count?	☐ 0 – 50,000 ☐ 50,001 – 100,000 ☐ 100,001 – 250,000	☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000 ☐ Over 1,000,000
Of your estimated total record count how many include the following types of information? **Select all that apply:**		
PII: e.g. customer account information, social security numbers, driver's license numbers	☐ 0 – 50,000 ☐ 50,001 – 100,000 ☐ 100,001 – 250,000	☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000 ☐ Over 1,000,000
PHI: Healthcare records	☐ 0 – 50,000 ☐ 50,001 – 100,000 ☐ 100,001 – 250,000	☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000 ☐ Over 1,000,000
PCI: Credit card information	☐ 0 – 50,000 ☐ 50,001 – 100,000 ☐ 100,001 – 250,000	☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000 ☐ Over 1,000,000
Biometric: An individual's unique physical or behavioral characteristics.	☐ 0 – 50,000 ☐ 50,001 – 100,000 ☐ 100,001 – 250,000	☐ 250,001 – 500,000 ☐ 500,001 – 1,000,000 ☐ Over 1,000,000
• **If you process credit card transactions, are you PCI Compliant?**	☐Yes ☐ No ☐ N/A If N/A is selected, the next question disappears.	
• **If yes, what is your PCI Merchant Level?**	☐ 1 ☐ 2 ☐ 3 ☐ 4	

Cybersecurity Controls and Procedures

Please affirm that the applicant's cybersecurity controls and procedures meet or exceed the following minimum cybersecurity standards:

- MFA is required for all admin access (remote and on-network) AND any remote access
- Have Endpoint Detection and Response (EDR) solution in place that covers 100% of their environment (example: CrowdStrike, Carbon Black or similar solution)
- Back-up critical information at least monthly
- Maintain a Recovery Time Objective (RTO) for critical systems, applications, and processes of 10 days or less
- Have a formal 30-day patching cadence, with critical and zero-day patching applied within 7 days

☐ **Yes, I affirm**

To receive a quote, you may either upload an application or answer the following additional questions in the Portal

Ransomware: Governance

Does the applicant employ any of the following solutions? **Select all that apply:**	
SPF (Sender Policy Framework)	☐ Yes ☐ No
DKIM (DomainKeys Identified Mail)	☐ Yes ☐ No
DMARC (Domain-based Message Authentication, Reporting and Conformance)	☐ Yes ☐ No
Do you have a Security Operations Center (SOC) or utilize a Managed Security Service Provider? • If yes, is it monitored 24/7?	☐ Yes ☐ No ☐ Yes ☐ No
Does the applicant have any End-of-Life software or systems present in their environment? If yes, indicate additional controls in place to secure these: • Extended support purchased • Application Whitelisting Enabled • Systems Segmented • Internet access disabled • Does the applicant conduct mandatory information security, phishing and privacy training of employees and contractors at least quarterly?	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
Does the applicant conduct mandatory information security, phishing and privacy training of employees and contractors at least quarterly?	☐ Yes ☐ No

Ransomware: Training

Are phishing simulations conducted for all employees?	☐ Yes ☐ No
Does applicant have report phishing email add-in enabled for all email users?	☐ Yes ☐ No
Does the applicant employ a sandboxing solution for investigating suspicious emails/attachments?	☐ Yes ☐ No

Ransomware: Backups

Which of the following does the applicant utilize for backups? • Tapes • Disks • Cloud	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
Where are backups stored? Select all that apply • MSSP • On premises • Offline storage • Offsite storage • Secondary data center	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No

Are Backups subject to the following measures? • MFA • Segmentation • Immutable • Virus / Malware scanning • Encryption	☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No
Unique backup credentials stored separately from other user credentials?	☐ Yes ☐ No
How frequently are backups made to offsite or offline storage? At least:	☐ Daily ☐ Weekly ☐ Monthly ☐ Quarterly
Is full recovery from a backup tested at least annually?	☐ Yes ☐ No

Ransomware: Recovery Time & Impact

Have these RTOs been validated in the last 12 months?	☐ Yes ☐ No
In the event Critical Information, or critical systems, applications or processes became unavailable, how long would it take to materially interrupt the applicant's business? At most:	☐ Under 1 Hour ☐ 1 – 8 Hours ☐ 8 – 12 Hours ☐ 12 – 24 Hours ☐ 24 – 48 Hours