**General Organization Information**

* How many people are employed at your organisation?
* What percentage of your staff work remotely for a significant proportion of their time?

**Privacy and Compliance**

* Are you required to be compliant with the GDPR or similar privacy legislation (E.g., HIPAA, CCPA, POPI, or PDPA)?
* Does any of the required legislation require the organisation to report a breach to a legislative body?
* Does any of the required legislation require you to report a breach to any affected parties?
* Which of these acts are you required to comply with (tick all that apply)? (Options include GDPR, HIPAA, CCPA, POPI, Australian Privacy Act, Brazil LGPD, Canada PIPEDA, Japan APPI, South Korea PIPA, Other.)

**Sensitive Data Handling**

* Aside from standard financial information do you (as any other High risk Protected information about clients/other) (E.g. Health information, information about minors, criminal records etc)?
* Do you maintain any sensitive government information?
* Do you hold significant confidential information belonging to the organisation that would be commercial value to competitors or other companies (E.g. IP, Contract information, Financial information etc)?

**Impact Risk Assessment**

* The following questions relate to the impact of specific cyber events on the business. For each event you should consider: operational, financial, reputational, and compliance impact.

For each of the following scenarios, you are asked to assess the impact in three categories (Financial, Reputational, Compliance) with the options: No Effect, Effect, No Impact, Impact.

* The ability for systems or data to be unavailable or inaccessible for a period of time.
* A cyber event e.g. ransomware/malware causing loss of internal data.
* A cyber event e.g. ransomware/malware causing loss of customer data.
* A cyber event e.g. ransomware/malware causing loss of third-party data.
* A cyber event resulting in the loss of confidential information.

**Incident History**

* To what extent have you experienced any data privacy incident or security incidents in the last 5 years?

These questions collectively assess your organization's risk profile, compliance requirements, sensitive data handling, and the potential impact of various cyber events.

**Cyber Risk Assessment**

* Has your organization performed a Cyber Risk Assessment?
* Was the risk assessment done internally?
* Please provide a copy of the assessment report if available.
* When was the last risk assessment done?
* Does your organization maintain a cyber risk register?
* Please upload a copy of the latest risk register.
* When was the risk register last updated?
* Have you specifically considered the risks posed to your cyber security by 3rd party contractors?

**Password Policy**

* Do you have a Password Management policy for access to your organization's platforms, applications and databases?
* Has this been reviewed within the last calendar year?
* Please supply a copy of the latest Policy.
* Which of these are required by your password policy (or if no policy the key systems your employees access e.g. email, ERP, shared systems):
  + Minimum Length >=8
  + Minimum Length >=12
  + Required Mixed Case
  + No Repeated Digits
  + Require Special Case Characters
  + Maximum number of repeated characters or digits
  + No repeated passwords within X changes
  + Passwords must be changed within a fixed period (No greater than 120 days)
  + Proprietary Complexity Algorithm (E.g. Google)
  + Two Factor Authentication
* Do you require Multi Factor Authentication for Email/Cloud Storage?
* Do you require Multi Factor Authentication for remote access or VPN access?
* In general is the access to critical systems managed via a single sign on platform (E.g. Active Directory)?

**Encryption**

* Is all data encrypted in transit, to and from the Internet?
* Is all data encrypted in transit within the organisation (including LAN/MPLS/BVPN etc)?
* Tick any of the below that reflect the way in which encryption keys are managed in your organisation.
* Is all company data encrypted at rest?

**Anti Virus**

* Does your organization require antivirus software on all endpoints and servers?
* Does your organization require anti malware software on all endpoints and servers?
* Does the organization make use of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) or any other automated security intervention technologies?
* Please provide details of the (IDS/IPS) technologies you use.
* Which of the below best describes how Antivirus alerts are monitored?

**Access Control Management and Network Security**

* Does your company have an access control policy for granting, revoking, handling and documenting access control procedures? (copy)
* Has the policy been reviewed in the last 12 Months?
* Please provide a copy of the access control policy.
* Does your company have a remote access policy dictating how and when users are able to access company data remotely?
* Has the policy been reviewed in the last 12 Months?
* Please provide a copy of the remote access policy.
* Provide detail of the extent your organisation makes use of access control tools such as IAM/MFA/BI0.
* Does the organisation make use of network segmentation and/or VLANs to limit access to resources and limit breach impact?

**Awareness Training**

* Does each user receive at a minimum annual awareness training around cyber security best practice and risks?
* Provide evidence of the training (for example training schedules and attendance records).
* Does each user receive period training in the form of mailers/gamification etc. around cyber awareness?
* Provide evidence of the training (for example schedules and system info).
* Does the company conduct annual (or more frequent) phishing engagements to test staff awareness?
* Provide evidence of the tests.
* Is training conducted in-house or by a third party?
* Do you measure employee engagement with the training?
* What methods do you use to assess their retention of the information?

**Vulnerability Management**

* Does each user receive at a minimum annual awareness training around cyber security best practice and risks?
* Provide evidence of the training (for example training schedules and attendance records).
* Does each user receive period training in the form of mailers/gamification etc. around cyber awareness?
* Provide evidence of the training (for example schedules and system info).
* Does the company conduct annual (or more frequent) phishing engagements to test staff awareness?
* Provide evidence of the tests.
* Is training conducted in-house or by a third party?
* Do you measure employee engagement with the training?
* What methods do you use to assess their retention of the information?

**Disaster Recovery and Business Continuity**

* Do you have documented Disaster Recovery policies or procedures?
* Has the policy been updated in the last 12 months?
* Please provide a copy of the policy.
* Is the plan tested at least annually via restore exercises or similar?
* Is the restored data user tested for performance and availability?
* Do you have a documented Business Continuity Plan?
* Has the policy been updated in the last 12 months?
* Please provide a copy of the policy.
* Is this policy tested at least annually via table-top exercises or similar?
* Do you have an Cyber Incident Response Plan that guides both end users and I.T. staff around how an incident should be handled?
* Has the policy been updated in the last 12 months?
* Please provide a copy of the policy.
* Is this policy tested at least annually via table-top exercises or similar?
* Does your organisation undergo penetration testing?
* Is this done at least annually?
* Is this testing done by an independent third party?
* Is the third party appropriately utilized/accredited/certified?
* Does the engagement test both internal (LAN) and external (WAN) resources?
* Is report management taking place to ensure findings are remediated swiftly?

**Security Framework and Information Management Security Systems**

* Do you currently use a security framework or ISMS?
* Which of these is the primary framework/ISMS you are following?
* Which of these best describes the current status of your organization with respect to the above standard?
* Please provide evidence of your current status (Either certificate or most recent assessment report)
* How often do you review and update your security policies and controls?
* Please provide a description of how policy reviews are managed in your organization.
* Do you have specific procedures for measuring the impact of third party contractors on your cyber security risk profile?
* Briefly describe these procedures...

**Security, Incident and Event Management**

* Does the organisation use tools or technology to detect breach attempts or attacks?
* Briefly describe these tools/technologies.
* As described above these include:
  + Security, Incident and Event Management (SIEM)
  + Security operations Centre (SOC)
  + Other
* Are your solutions:
* Do you require any assistance from Moore Global in meeting the required minimum standards?