CLOUD SECURITY CHECK LIST

SOURCE VERIFICATION

- [ ] Verify that the software/cloud provider is well recognized in the legal and business communities.

ENCRYPTION AND VIRUS PROTECTION

- [ ] Ensure that all data is encrypted in-transit and at-rest.
- [ ] Implement centrally-managed virus protection for desktops and cloud servers.
- [ ] Implement systems specifically designed to detect and prevent ransomware.

FIREWALL AND THREAT MONITORING

- [ ] Implement active firewall protection at client-side and server/application side.
- [ ] Ensure cloud/software provider monitors 24x7 for threats including failed logins and known attack patterns.

SUBPOENA POLICY AND MULTI-FACTOR AUTHENTICATION

- [ ] Ensure cloud/software provider has a written policy if served with a subpoena regarding your data.
- [ ] Ensure cloud/software provider segregates clients (firms) at server and/or network level.

NIST FRAMEWORK AND DATA OWNERSHIP

- [ ] Ensure your cloud/software provider has adopted and administers NIST security framework including password rules and security policies.
- [ ] Understand your cloud/software provider's contract regarding data ownership, ensure your data remains your property.

PHYSICAL ACCESS AND DATA SOVEREIGNTY

- [ ] Ensure physical safeguards are in place at your cloud/software provider's data center.
- [ ] Ensure that your cloud/software provider keeps your firm data, including backups, in the continental US.
- [ ] Encrypted communications, policy, and training:

IMPLEMENT SECURE/ENCRYPTED EMAIL

- [ ] Adopt encrypted communication/chat applications such as Microsoft Teams or Slack.
- [ ] Train employees on how to follow security-best practices.
- [ ] Implement BYOD policies and security measures.
- [ ] Permissions/access control and regular security reviews:
- [ ] Implement and routinely review permissions to files and data within your cloud software.
- [ ] Consider adopting a 'Least Privilege' approach to data access.
- [ ] Conduct regular reviews of all data security processes, policies, systems, hardware, and software.
- [ ] Consider third-party security reviews.
- [ ] Create and document a response plan for data breaches or other security incidents.
- [ ] Review and revise at least annually.

DATA BACKUP AND DISASTER RECOVERY

- [ ] Ensure that your cloud/software provider has a comprehensive data backup and disaster recovery plan in place.
- [ ] Verify that backups are encrypted, regularly tested, and stored offsite in secure locations.

DATA RETENTION AND DESTRUCTION POLICY:

- [ ] Create and document a data retention and destruction policy to ensure that data is only kept for as long as it is necessary.
- [ ] Ensure that all data is securely and irreversibly destroyed when it is no longer needed.

AUDITING AND LOGGING

- [ ] Ensure that your cloud/software provider maintains audit logs for all activities within your cloud environment.
- [ ] Review audit logs regularly to detect suspicious activities and take corrective actions.

COMPLIANCE AND REGULATIONS

- [ ] Ensure that your cloud/software provider complies with industry-specific regulations and standards such as HIPAA, GDPR, and PCI DSS.
- [ ] Review compliance certifications and reports regularly.

THIRD-PARTY VENDOR MANAGEMENT

- [ ] Ensure that your cloud/software provider conducts background checks and assessments on all third-party vendors before granting them access to your data.
- [ ] Review third-party vendor agreements to ensure they adhere to your security policies.

SECURE CODING PRACTICES

- [ ] Ensure that your cloud/software provider follows secure coding practices when developing new software or applications.
- [ ] Conduct regular code reviews to identify and fix vulnerabilities.
- [ ] Incident response testing:
- [ ] Test your incident response plan regularly to ensure that it is effective and up-to-date.
- [ ] Conduct tabletop exercises and simulated attacks to identify gaps and improve response times.

USER ACCESS MANAGEMENT

- [ ] Implement strong user access controls to ensure that users only have access to data and systems that they need to do their jobs.
- [ ] Use least privilege principles to grant access and enforce strong password policies.

NETWORK SEGMENTATION

- [ ] Implement network segmentation to isolate sensitive data and applications from less sensitive data and systems.
- [ ] Limit access between segments and enforce access controls to reduce the risk of lateral movement in case of a security breach.

VULNERABILITY MANAGEMENT

- [ ] Regularly scan your cloud environment for vulnerabilities and prioritize remediation based on the severity of the risk.
- [ ] Patch and update software and systems regularly to ensure that known vulnerabilities are mitigated.

SECURITY INCIDENT RESPONSE

- [ ] Ensure that your security incident response plan includes clear procedures for responding to security incidents.
- [ ] Train all employees on how to identify and report security incidents, and ensure that all incidents are tracked and documented.

DISASTER RECOVERY TESTING

- [ ] Test your disaster recovery plan regularly to ensure that it is effective and that critical systems can be recovered in the event of a disaster.
- [ ] Update the plan regularly based on changes to your cloud environment.

SECURITY AWARENESS TRAINING

- [ ] Train all employees on basic security awareness topics such as phishing, password hygiene, and social engineering attacks.
- [ ] Provide regular updates and refreshers to keep employees informed and vigilant.