Policy Name:	Risk Assessment Policy				
Revision #:	0.9	**Effective:**	January 1, 2024	**Page**	1 of 1

1.0 PURPOSE

This policy describes how the organization evaluates and manages risk.

2.0 SCOPE

This policy applies to all mission critical technology systems, vendors, and suppliers, including the Microsoft Office 365.

3.0 POLICY

3.1 Risk Assessment

The firm will regularly identify and track risks and will review each non-mitigated risk on an annual basis. Identifying risks means looking to uncover any threats and vulnerabilities in the organization's systems. If risks are found, they will be tracked and evaluated by firm leadership. Issues will be addressed with a mitigation plan within an agreed upon timeframe and a risk register will be maintained.

Risk assessment techniques may include:

- Comparing Office 365 security settings against guidelines published by the Center for Internet Security (CIS)
- Conducting a third-party risk assessment of the organization's technology partners and vendors (TPRM)
- Vulnerability scanning
- Penetration testing

4.0 RELEVANT NIST CONTROLS

Control	Control Description	Document Section
NIST 800-171 3.11.1	Risk Assessment - Periodically assess the risk to company operations	Entire Document

5.0 REVISION HISTORY

Date	Name	Changes Made	Revision #
10/25/2023	Frank Schipani	Initial draft created	0.9
12/30/2023	Audit Committee	Approved Policies	