

## Company A Risk Analysis

Company A performed an internal risk analysis in anticipation of system integration with Company B. This risk analysis was performed in accordance with NIST SP 800-30 Rev 1 to identify the following:

- vulnerabilities
- risk likelihood

Table A. Risk Classifications

<b>Risk Level</b>	<b>Description</b>
High	The loss of confidentiality, integrity, or availability may be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability may be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
Low	The loss of confidentiality, integrity, or availability may be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Table B. Data Sensitivity

<b>Type of Data</b>	<b>Sensitivity</b>		
	<b>Confidentiality</b>	<b>Integrity</b>	<b>Availability</b>
Customer PII (e.g., Account Numbers, Social Security Numbers, and Phone Numbers)	High	High	Moderate
Employee PII (e.g., Social Security Numbers and Employee Identification Numbers)	High	High	Moderate
Company intellectual property (e.g., credit scoring calculations)	High	High	Moderate
Marketing and advertising	Moderate	Moderate	Low



Table C. System Inventory

System Components	
Servers	Windows server 2019; role: internal SharePoint server Windows server 2019; role: Exchange server Windows server 2012; role: Application server Windows server 2012R2; File server DMZ Windows server 2012; role: FTP and external Web Server
Workstations	75 - Windows 10 Pro 20 - configured for remote desktop access
Switches	4 - Cisco 3750X
Firewall	Fortinet 800D NGFW
Border router	Cisco 7600
Laptops	14 - Windows 7 6 - Windows 11
Wireless Access Points	2 - Meraki M28
Cable plant	Cat5e

Table D. Risk Identification

Risk #	Vulnerability	Risk Likelihood
1	Open ports 21-90, 3389	High
2	All users use eight-character passwords	High
3	User accounts no longer required are not removed	Moderate
4	All users have local administrative privileges	Moderate
5	Regular password changes are not enforced	Moderate
6	End-of-Life Equipment in use	Low

