**Company A Risk Analysis**

Company A performed this risk assessment in anticipation of system integration with Company B. This risk assessment was performed in accordance with a methodology described in NIST 800-30 to identify the following:

• vulnerabilities

• risk likelihood

Table A. Risk Classifications

|  |  |
| --- | --- |
| **Risk Level** | **Description** |
| 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

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Data** | **Sensitivity and Likelihood** | | |
| **Confidentiality** | **Integrity** | **Availability** |
| Customer PII | High | High | Moderate |
| Insurance underwriting | High | High | High |
| Employee PII | High | High | Moderate |
| Company intellectual property | High | High | Moderate |
| Marketing and advertising | Moderate | Moderate | Low |

Table C. System Inventory

|  |  |
| --- | --- |
| **System Components** | |
| Servers | Windows server 2012; role: web server  Windows server 2008; role: exchange  Windows server 2008; role: application  Windows server 2012; role: data storage cluster  DMZ Windows server 2012; role: FTP |
| Workstations  #86 | Windows 10 Pro  Six configured for remote desktop at ports 88–93 |
| Switches | HCC: four Cisco 2960 48/4  VCC: three Cisco 2960 24/4 |
| Fire wall | Cisco PIX 515E |
| Border router | Cisco 2811 |
| Laptops | Dell Inspiron, i5-4310M CPU @ 2.70GHz  Mixture of Windows 7(14) and Windows 10(6) |
| Cable plant | Cat5e |

Table D. Risk Identification

|  |  |  |
| --- | --- | --- |
| **Risk #** | **Vulnerability** | **Risk Likelihood** |
| 1 | Open ports 88–93 | High |
| 2 | User accounts no longer required are not removed | Moderate |
| 3 | Full access privileges are granted to every employee with exception to the payroll system | Moderate |
| 4 | Regular password changes are not enforced | Moderate |
| 5 | Cisco PIX 515E fire wall | Moderate |