Acquisition Assessment Policy

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: Updated and converted to new format June 2014

1. Overview

The process of integrating a newly acquired company can have a drastic impact on the security poster of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

- Assess company's security landscape, posture, and policies
- Protect both <Company Name> and the acquired company from increased security risks
- Educate acquired company about <Company Name> policies and standard
- Adopt and implement <Company Name> Security Policies and Standards
- Integrate acquired company
- Continuous monitoring and auditing of the acquisition

2. Purpose

The purpose of this policy is to establish Infosec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an Infosec acquisition assessment.

3. Scope

This policy applies to all companies acquired by <Company Name> and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

4. Policy

4.1 General

Acquisition assessments are conducted to ensure that a company being acquired by <Company Name> does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The Infosec Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Infosec role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to <Company Name>'s networks. Below are the minimum requirements that the acquired company must meet before being connected to the <Company Name> network.

4.2 Requirements

4.2.1 Hosts

4.2.1.1 All hosts (servers, desktops, laptops) will be replaced or re-imaged with a <Company Name> standard image or will be required to adopt the minimum standards for end user devices.

4.2.1.2 Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by Infosec.

4.2.1.3 All PC based hosts will require <Company Name> approved virus protection before the network connection.

4.2.2 Networks

4.2.2.1 All network devices will be replaced or re-imaged with a <Company Name> standard image.

4.2.2.2 Wireless network access points will be configured to the <Company Name> standard.

4.2.3 Internet

4.2.3.1 All Internet connections will be terminated.

4.2.3.2 When justified by business requirements, air-gapped Internet connections require Infosec review and approval.

4.2.4 Remote Access

4.2.4.1 All remote access connections will be terminated.

4.2.4.2 Remote access to the production network will be provided by <Company Name>.

4.2.5 Labs

4.2.5.1 Lab equipment must be physically separated and secured from non-lab areas.

4.2.5.2 The lab network must be separated from the corporate production network with a firewall between the two networks.

4.2.5.3 Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Lab Security Group (LabSec).

4.2.5.4 All acquired labs must meet with LabSec lab policy, or be granted a waiver by LabSec.

4.2.5.5 In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the <Company Name> Chief Information Officer (CIO) must acknowledge and approve of the risk to <Company Name>'s networks

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Business Critical Production Server

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.