Risk Assessment Policy

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: *Retired*

1. Overview

See Purpose.

2. Purpose

To empower Infosec to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

3. Scope

Risk assessments can be conducted on any entity within <Company Name> or any outside entity that has signed a *Third Party Agreement* with <Company Name>. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

4. Policy

The execution, development and implementation of remediation programs is the joint responsibility of Infosec and the department responsible for the system area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Infosec Risk Assessment Team in the development of a remediation plan.

For additional information, go to the *Risk Assessment Process*.

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

- Risk Assessment Process
- Third Party Agreement

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Converted to new format and retired

