# Risk Assessment Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The quality and integrity of [Company Name’s] risk assessments are used to determine the likelihood and magnitude of harm that could come to an information system and ultimately [Company Name] itself in the event of a security breach. By determining the amount of risk that exists, [Company Name] will be in a better position to determine how much of that risk should be mitigated and what controls should be used to achieve that mitigation. Without risk assessments, the potential exists that the organization can leverage inappropriate (either too strict or too lax) security controls to protect information systems.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

The Risk Assessment Policy applies to all employees of [Company Name], including all temporary or contract workers. Specifically, it includes:

* Mainframes, servers, and other devices that provide centralized computing capabilities.
* SAN, NAS, and other devices that provide centralized storage capabilities.
* Desktops, laptops, and other devices that provide distributed computing capabilities.
* Routers, switches, and other devices that provide network capabilities.
* Firewalls, IDP sensors, and other devices that provide dedicated security capabilities.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

1. Risk assessments will be performed on all information systems that house or access [Company Name] controlled information. These assessments will address unauthorized access, use, disclosure, disruption, modification, and/or destruction of information or the information system itself. Further, the assessments shall identify known potential threats, the likelihood of their occurrence, and the magnitude of the impact of those threats should they occur.
2. Risk assessments shall be performed upon initial acquisition of an information system (in the event that the information system is owned/operated by [Company Name]) or prior to initial establishment of service agreements or in the event that the information system is owned/operated by a third party on behalf of [Company Name]). Further, the risk assessment shall be reviewed and, where required, updated after [indicate interval – suggest three years] or whenever a significant change is made to the information system, whichever comes first.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Determine the amount and nature of risk to which a system is exposed:

* + - * + Collect and document the information that defines the system.
				+ Identify and document all potential sources of threat to which the system could be exposed and, for those threats, identify and document all potential vulnerabilities:

*Use vulnerability sources such as the* [*National Vulnerability Database*](http://nvd.nist.gov/)*.*

*Use outputs from System Security Tests.*

* + - * + Identify and document all implemented controls that are intended to have a mitigating effect on threats and vulnerabilities:

*Evaluate both Technical (access control systems, firewalls, etc.) and Non-Technical (policies and procedures) controls.*

*Evaluate both Detective (those that warn of violations) and Preventative (those that inhibit violations) controls.*

* + - * + Estimate the likelihood that a particular vulnerability will occur in the face of controls that may be in place to mitigate it:

*High likelihood indicates the threat-source is motivated and capable and controls are insufficient or ineffective.*

*Medium likelihood indicates the threat-source is motivated and capable but that controls may be sufficient and effective.*

*Low likelihood indicates the threat-source is motivated and capable but that controls are sufficient and effective* ***OR*** *the threat-source is unmotivated or incapable.*

* + - * + Estimate the impact that a particular vulnerability will have if exercised in the face of controls that may be in place to mitigate it:

*High impact indicates significant loss of assets or resources, significant damage to the organizational mission, or serious human injury or death.*

*Medium impact indicates moderate loss of assets or resources, moderate damage to the organizational mission, or human injury.*

*Low impact indicates minimal loss of assets or resources or minimal damage to the organizational mission.*

* + - * + Cross reference the determined likelihood with the determined impact to define the overall risk of each vulnerability. Decide if the risk level is to be accepted and, if not, to what degree it is to be mitigated:

*Very High risk constitutes high likelihood and high impact. Risks of this nature have the strongest need for corrective action and resolution should be considered an emergency action and undertaken immediately.*

*High risk constitutes high likelihood and medium impact or medium likelihood and high impact. Risks of this nature have a strong need for corrective action and a corrective response plan must be developed and put in place within 30 days.*

*Medium risk constitutes high likelihood and low impact, low likelihood and high impact, or medium likelihood and medium impact. Risks of this nature have a moderate need for corrective action and a corrective response plan must be developed and put in place within 90 days.*

*Low risk constitutes medium likelihood and low impact or low likelihood and medium impact. Risks of this nature have a low need for corrective action and a corrective response plan must be developed and put in place within 180 days.*

*Very Low risk constitutes low likelihood and low impact. Risk of this nature can be considered negligible and no corrective response plan is required. However, the risk should be reassessed annually to determine if the risk level has been elevated.*

* + - * + Identify and evaluate additional controls that will reduce the identified risk to acceptable levels:

*Evaluate both Technical (access control systems, firewalls, etc.) and Non-Technical (policies and procedures) controls.*

*Evaluate both Detective (those that warn of violations) and Preventative (those that inhibit violations) controls.*

*Perform a cost-benefit analysis for each control to narrow the selection of controls to those that mitigate risk cost effectively.*

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.