Risk Assessment Policy

ACME Evil Anvil Corporation

March 2019

Contents

1 Purpose and Scope **2**

2 Background **2**

3 References **2**

4 Policy **2**

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document

1 Purpose and Scope

a. The purpose of this policy is to define the methodology for the assessment and treatment of information security risks within the organization, and to define the acceptable level of risk as set by the organization's leadership.

b. Risk assessment and risk treatment are applied to the entire scope of the organization's information security program, and to all assets which are used within the organization or which could have an impact on information security within it.

c. This policy applies to all employees of the organization who take part in risk assessment and risk treatment.

2 Background

a. A key element of the organization's information security program is a holistic and systematic approach to risk management. This policy defines the requirements and processes for the organization to identify information security risks. The process consists of four parts: identification of the organization's assets, as well as the threats and vulnerabilities that apply; assessment of the likelihood and consequence (risk) of the threats and vulnerabilities being realized, identification of treatment for each unacceptable risk, and evaluation of the residual risk after treatment.

3 References

a. Risk Assessment Report Template

4 Policy

a. *Risk Assessment*

   i. The risk assessment process includes the identification of threats and vulnerabilities having to do with company assets.

   ii. The first step in the risk assessment is to identify all assets within the scope of the information security program; in other words, all assets which may affect the confidentiality, integrity, and/or availability of information in the organization. Assets may include documents in paper or electronic form, applications, databases, information technology equipment, infrastructure, and external/outsourced services and processes. For each asset, an owner must be identified.

iii. The next step is to identify all threats and vulnerabilities associated with each asset. Threats and vulnerabilities must be listed in a risk assessment table. Each asset may be associated with multiple threats, and each threat may be associated with multiple vulnerabilities. A sample risk assessment table is provided as part of the Risk Assessment Report Template (reference (a)).

iv. For each risk, an owner must be identified. The risk owner and the asset owner may be the same individual.

v. Once risk owners are identified, they must assess:

   1. Consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes.

   2. Likelihood of occurrence of such a risk (i.e. the probability that a threat will exploit the vulnerability of the respective asset).

   3. Criteria for determining consequence and likelihood are defined in Tables 3 and 4.

vi. The risk level is calculated by adding the consequence score and the likelihood score.

Consequence Level	**Consequence Score**	**Description**
Low	0	Loss of confidentiality, integrity, or availability will not affect the organization's cash flow, legal, or contractual obligations, or reputation.
Moderate	1	Loss of confidentiality, integrity, or availability may incur financial cost and has low or moderate impact on the organization's legal or contractual obligations and/or reputation.
High	2	Loss of confidentiality, integrity, or availability will have immediate and or/considerable impact on the organization's cash flow, operations, legal and contractual obligations,and/ or reputation.

Table 3: Description of Consequence Levels and Criteria

Likelihood Level	Likelihood Score	Description
Low	0	Either existing security controls are strong and have so far provided an adequate level of protection, or the probability of the risk being realized is extremely low. No new incidents are expected in the future.
Moderate	1	Either existing security controls have most provided an adequate level of protection or the probability of the risk being realized is moderate. Some minor incidents may have occured. New incidents are possible, but not highly likely.
High	2	Either existing security controls are not in place or ineffective; there is a high probability of the risk being realized. Incidents have a high likelihood of occuring in the future.

Table 4: Description of Likelihood Levels and Criteria

b. *Risk Acceptance Criteria*

   i. Risk values 0 through 2 are considered to be acceptable risks.

   ii. Risk values 3 and 4 are considered to be unacceptable risks. Unacceptable risks must be treated.

c. *Risk Treatment*

   i. Risk treatment is implemented through the Risk Treatment Table. All risks from the Risk Assessment Table must be copied to the Risk Treatment Table for disposition, along with treatment options and residual risk. A sample Risk Treatment Table is provided in reference (a).

   ii. As part of this risk treatment process, the CEO and/or other company managers shall determine objectives for mitigating or treating risks. All unacceptable risks must be treated. For continuous improvement purposes, company managers may also opt to treat other risks for company assets, even if their risk score is deemed to be acceptable.

   iii. Treatment options for risks include the following options:

      1. Selection or development of security control(s).

2. Transferring the risks to a third party; for example, by purchasing an insurance policy or signing a contract with suppliers or partners.
3. Avoiding the risk by discontinuing the business activity that causes such risk.
4. Accepting the risk; this option is permitted only if the selection of other risk treatment options would cost more than the potential impact of the risk being realized.

iv. After selecting a treatment option, the risk owner should estimate the new consequence and likelihood values after the planned controls are implemented.

d. *Regular Reviews of Risk Assessment and Risk Treatment*

i. The Risk Assessment Table and Risk Treatment Table must be updated when newly identified risks are identified. At a minimum, this update and review shall be conducted once per year. It is highly recommended that the Risk Assessment and Risk Treatment Table be updated when significant changes occur to the organization, technology, business objectives, or business environment.

e. *Reporting*

i. The results of risk assessment and risk treatment, and all subsequent reviews, shall be documented in a Risk Assessment Report.