Cyber Risk Assessment Policy

ACME Evil Anvil Corporation

September 2020

Contents

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 procedures to assess and treat information security risks within the organization, and to define the acceptable level of risk overall.

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

c. This policy applies to all management and employees that take part in the organization's risk assessments. This policy must be made readily available to all whom it applies to.

2 Background

a. This policy defines a step-by-step process for conducting risk assessments, as well as to treat identified risks from an information security perspective. This policy also describes how to prepare the Risk Assessment Report required as part of the risk assessment process.

b. When conducting a risk assessment, the organization must identify all organizational information systems . It must then identify all threats and vulnerabilities having to do with such systems , and rate the severity of such threats and vulnerabilities according to a predefined rating scale. Asset and risk owners must be defined for each risk item.

c. Once the risk assessment is completed, the organization shall determine how to manage risks where the overall assessed risk rating is deemed as too high. This management is known as risk treatment. Risk treatment options include but are not limited to applying security controls, outsourcing risk, accepting risk, or discontinuing the activity associated with the risk.

d. A penetration test must be performed by a third party to verify the accuracy of the risk assessment and effectiveness of deployed risk treatments.

3 Procedure To Execute Risk Assessment Report

a. Confirms that the entire risk assessment and risk treatment process has been carried out according to the Risk Assessment Policy.

b. The purpose of the risk assessment was to identify all information systems their vulnerabilities, and threats that could exploit vulnerabilities. These

parameters were further evaluated in order to establish the criticality of individual risks.

c. The purpose of the risk treatment was to define the systematic means of reducing or controlling the risks identified in the risk assessment.

d. All risk assessment and treatment activities were completed within the scope of the organization's information security program.

e. The risk assessment was implemented in the period from [day/month/year] to [day/month/year]. The risk treatment was implemented from [day/month/year] to [day/month/year]. Final reports were prepared during [specify period].

f. The risk assessment and risk treatment process was managed by [person responsible for managing the risk assessment process] with expert assistance provided by [person or company responsible for assistance].

g. During the risk assessment, information was collected through questionnaires and interviews with responsible persons, namely the asset owners across organizational units.

h. The process was conducted as follows:

   i. All information systems and their owners were identified.

   ii. Threats were identified for each asset, and corresponding vulnerabilities were identified for each threat.

   iii. Risk owners were identified for each risk.

   iv. Consequences of the loss of confidentiality, integrity and availability were evaluated using a score from 0 to 2, with 0 being the lowest rating and 2 being the highest rating.

   v. The likelihood of risk occurrence (i.e. that the threat will exploit the vulnerability) was evaluated using a score from 0 to 2, with 0 being the lowest rating and 2 being the highest rating.

   vi. The level of risk was calculated by adding up the consequence and likelihood.

   vii. Risks with a score of 3 or 4 were determined to be unacceptable risks.

   viii. For each unacceptable risk, a risk treatment option was considered, and appropriate information security controls were selected.

   ix. After controls were applied, residual risks were assessed.

i. The following documents were used or generated during the implementation of risk assessment and risk treatment:

i. Risk Assessment Table (Appendix A): for each combination of systems , vulnerabilities and threats, this table shows the values for consequence and likelihood, and calculates the risk.

ii. Risk Treatment Table (Appendix B): defines the options for risk treatment, selection of controls for each unacceptable risk, and the level of residual risk.