Risk Assessment Policy

BritePool

January 2020

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC9.1

Table 2: Document history

Date	Comment
Jan 2 2020	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. Impact 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 impact and likelihood are defined in Tables below.

vi. The risk level is calculated by X the impact score and the likelihood score. TODO: REPLACE X with something.

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 1: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

Qualitiative	**Semi-Quantitiative**	**Description**		**Values**	**Values**	
Very High	96-100	10	Adversary is almost certain to initiate the threat event.			
High	80-95	8	Adversary is highly likely to initiate the threat event.			
Moderate	21-79	5	Adversary is somewhat likely to initiate the threat event.			
Low	5-20	2	Adversary is unlikely to initiate the threat event.			
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event			

Table 2: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitiative	**Semi-Quantitiative**	**Description**		**Values**	**Values**	
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur;				or occurs more than 100 times per year.			
High	80-95	8				

Error, accident, or act of nature is highly likely to occur; | | | | | or occurs more than 10-100 times per year. | +————————+————————————+————————————————————————————+ | Moderate | 21-79 | 5 | Error, accident, or act of nature is somewhat likely to | | | | | occur; or occurs more than 1-10 times per year. | +————————+————————————+————————————————————————————+ | Low | 5-20 | 2 | Error, accident, or act of nature is unlikely to occur; or | | | | | occurs less than once a year but more than once every 10 yrs.| +————————+————————————+————————————————————————————+ | Very Low | 0-4 | 0 | Error, accident, or act of nature is highly unlikely to | | | | | occur; or occurs less than once every 10 yrs. | +————————+————————————+————————————————————————————+

Table 3: Likelihood of Threat Event Resulting in Adverse Impacts +————————+————————————+————————————————————————————+ | **Qualitiative**| **Semi-Quantitiative** | **Description** | | **Values** | **Values** | | +========================+============================+==========

| Very High | 96-100 | 10 | If the threat event is initiated or occurs, it is almost | | | | | certain to have adverse impacts. | +————————+————————————+————————————————————————————+ | High | 80-95 | 8 | If the threat event is initiated or occurs, it is highly | | | | | likely to have adverse impacts. | +————————+————————————+————————————————————————————+ | Moderate | 21-79 | 5 | If the threat event is initiated or occurs, it is somewhat | | | | | likely to have adverse impacts | +————————+————————————+————————————————————————————+ | Low | 5-20 | 2 | If the threat event is initiated or occurs, it is unlikely to| | | | have adverse impacts. | +————————+————————————+————————————————————————————+ | Very Low | 0-4 | 0 | If the threat event is initiated or occurs, it is highly | | | | | unlikely to have adverse impacts. | +————————+————————————+————————————————————————————+

Table 4: Assessment Scale – Overall Likelihood +————————-+————————————————————————————————————+ | **Likelihood of Threat Events Result in Adverse Impacts** | | **Likelihood Threat Event Initiation or Occurrence** | Very Low | Very Low | Moderate | High | Very High | +========================+=============+=============+=============+=============+

| Very High | Low | Moderate | High | Very High | Very High | +————————-+————-+————-+————-+————-+————-+ | High | Low | Moderate | Moderate | High | Very High | +————————-+————-+————-+————-+————-+————-+ | Moderate | Low | Low | Moderate | Moderate | High | +————————-+————-+————-+————-+————-+————-+ | Low | Very Low | Low | Low | Moderate | Moderate | +————————-+————-+————-+————-+————-+————-+ | Very Low | Very Low | Very Low | Low | Low | Low | +————————-+————-+————-+————-+————-+————-+

Table 5: Assessment Scale – Impact of Threat Events +————————

+——————+——————————————————+ | **Qualitiative**| **Semi-Quantitiative** | **Description** | | **Values** | **Values** | |
+==================+==========================+==========================+
| Very High | 96-100 | 10 | The threat event could be expected to have multiple severe | | | | | or catastrophic adverse effects on organizational operations,| | | | | organizational assets, individuals, other organizations, | | | | | or the Nation. | +——————+——————+——————————————————+ | High | 80-95 | 8 | The threat event could be expected to have a severe or | | | | | catastrophic adverse effect on organizational operations, | | | | | organizational assets, individuals, other organizations, or | | | | | the Nation. A severe or catastrophic adverse effect means | | | | | that, for example, the threat event might: (i) cause a severe| | | | | degradation in or loss of mission capability to an extent and| | | | | duration that the organization is not able to perform one or | | | | | more of its primary functions; (ii) result in major damage to| | | | | organizational assets; (iii) result in major financial loss; | | | | | or (iv) result in severe or catastrophic harm to individuals | | | | | involving loss of life or serious life threatening injuries. | +——————+——————+——————————————————+ | Moderate | 21-79 | 5 | The threat event could be expected to have a serious adverse | | | | | effect on organizational operations, organizational assets, | | | | | individuals other organizations, or the Nation. A serious | | | | | adverse effect means that, for example, the threat event | | | | | might: (i) cause a significant degradation in mission | | | | | capability to an extent and duration that the organization is| | | | | able to perform its primary functions, but the effectiveness | | | | | of the functions is significantly reduced; (ii) result in | | | | | significant damage to organizational assets; (iii) result in | | | | | significant financial loss; or (iv) result in significant | | | | | harm to individuals that does not involve loss of life or | | | | | serious life threatening injuries. | +——————+——————+——————————————————+ | Low | 5-20 | 2 | The threat event could be expected to have a limited adverse | | | | | effect on organizational operations, organizational assets, | | | | | individuals other organizations, or the Nation. A limited | | | | | adverse effect means that, for example, the threat event | | | | | might: (i) cause a degradation in mission capability to an | | | | | extent and duration that the organization is able to perform | | | | | its primary functions, but the effectiveness of the functions| | | | | is noticeably reduced; (ii) result in minor damage to | | | | | organizational assets; (iii) result in minor financial loss; | | | | | or (iv) result in minor harm to individuals. | +——————+——————+——————————————————+ | Very Low | 0-4 | 0 | The threat event could be expected to have a negligible | | | | | adverse effect on organizational operations, organizational | | | | | assets, individuals other organizations, or the Nation. | +——————+——————+——————————————————+

Table 6: Assessment Scale – Level of Risk +——————+——————+——————————————————+ | **Qualitiative**| **Semi-Quantitiative** | **Description** | | **Values** | **Values** | |

+==========+==========+==========+
| Very High | 96-100 | 10 | Threat event could be expected to have multiple severe or | | | | | catastrophic adverse effects on organizational operations, | | | | | organizational assets, individuals, other organizations, or | | | | | the Nation. |
+----------+----------+----------+
| High | 80-95 | 8 | Threat event could be expected to have a severe or | | | | | catastrophic adverse effect on organizational operations, | | | | | organizational assets, individuals, other organizations, or | | | | | the Nation. |
+----------+----------+----------+
| Moderate | 21-79 | 5 | Threat event could be expected to have a serious adverse | | | | | effect on organizational operations, organizational assets, | | | | | individuals, other organizations, or the Nation. |
+----------+----------+----------+
| Low | 5-20 | 2 | Threat event could be expected to have a limited adverse | | | | | effect on organizational operations, organizational assets, | | | | | individuals, other organizations, or the Nation. |
+----------+----------+----------+
| Very Low | 0-4 | 0 | Threat event could be expected to have a negligible adverse | | | | | effect on organizational operations, organizational assets, | | | | | individuals, other organizations, or the Nation. |
+----------+----------+----------+

Table 7: Assessment Scale - Level of Risk (Combination of Likelihood and Impact)

Likelihood	**Level of Impact**		**Threat Occurs**			**and Results in**			**Adverse Impact**	Very Low	Very Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

b. *Risk Acceptance Criteria*

   i. Risk values W through X are considered to be acceptable risks. TODO: DETERMINE W, X

   ii. Risk values Y and Z are considered to be unacceptable risks. Unacceptable risks must be treated. TODO: DETERMINE Y, Z

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.