The AET

Risk Assessment and Treatment Policy

Purpose and Scope

This Risk Assessment Policy guides The AET in performing risk assessments to account for threats, vulnerabilities, likelihood, and impact to The AET assets, team members, customers, vendors, suppliers, and partners based upon the The AET services considering security, availability, integrity, and confidentiality needs.

From time to time, The AET may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to The AET including applicable laws and regulations.

This policy applies to all The AET assets utilized by personnel acting on behalf of The AET or accessing its applications, infrastructure, systems, or data. All personnel are required to read, accept, and follow all The AET policies and plans.

Risk Assessment Framework

The AET conducts assessments of risk, which includes the likelihood and impact of risk from the unauthorized access, use, disclosure, disruption, modification and/or destruction of The AET systems, applications, infrastructure, and data pertaining to The AET's environment.

The risk assessment process is coordinated by Roger Hanagriff, which includes the identification and evaluation of assets, threats, and vulnerabilities. Assets should be identified by respective asset owners, and the assessment of threats as well as the likelihood and criticality of potential vulnerability exploitation, should be performed by respective risk owners.

A risk assessment may include a review of:

- internal controls including policies, procedures, business processes, and technical security safeguards
- human resource practices related to hiring, termination, and discipline procedures
- facility controls

- exposure to theft
- systems and applications used to collect, store, process or transmit confidential data

Risk Assessment Process

The risk assessment process should align with the following steps:

(1) Scoping Assets

In order to begin the risk assessment process, the assessor should determine the scope of what needs to be covered in the assessment. An effective assessment should be limited in its scope to the applicable assets.

Such scoping activities may include:

- Review inventory of critical system assets (hardware, software, facilities, etc.)
- Identification of data owners (electronic and non-electronic data)
- Identification of workforce members with access to stored data by hardware/software
- Mapping data flow through The AET and vendor systems
- Conducting an inventory of data storage (including non-electronic data)
- System characterization (e.g. essential, non-essential)

(2) Identifying Threats and Vulnerabilities

Vulnerabilities and the related threats, both internal and external, to The AET operations (including, but not limited to, its mission, functions, image, or reputation), assets, information, and individuals may be identified and documented as part of the The AET risk assessment.

Threat
A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, or other organizations, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. [SP 800-30 Rev.1]

Vulnerability

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [SP 800-30 Rev.1]

Vulnerabilities may be identified by the following:

- Vulnerability scanning and penetration tests
- Security control monitoring technologies
- Detected patterns, heuristics, or specific activities that indicate process gaps or technical weaknesses
- Internal and external audits
- External security vulnerabilities databases (e.g. CVE database) and reports

(3) Analyze Risks

For each risk, a risk owner has to be identified – the person or organizational unit responsible for each risk. This person may or may not be the same as the asset owner. Once risk owners have been identified, it is necessary to assess consequences for each combination of threats and vulnerabilities for an individual asset if such a risk materializes:

Initial (or Inherent) Risk Likelihood Determination
How likely will an identified threat or vulnerability impact the organization given existing security controls?

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).

Initial (or Inherent) Risk Impact Analysis
What is the cost if an identified threat or vulnerability impacts the organization given existing security controls?

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Initial (or Inherent) Risk Score

After the likelihood and impact analysis, a risk determination should be made. Risk is a function of the likelihood of a threat event's occurrence and potential adverse impact should the event occur. In order to determine risk score, The AET multiplies impact * likelihood. The higher number equates to higher potential risk.

(4) Risk Treatment

For any critical or high risks identified during the risk assessment process, The AET will immediately develop action plans to mitigate those risks which could include patching of vulnerable systems and/or applying other control activities. Risk responses shall consider obligations such as contractual agreements, laws, regulations and standards. The following items will have to be amended or defined based on discovered risk: IT policy and strategies, risk strategies, cost-effectiveness, type of protection, threats covered, risk levels, existing alternatives, and additional benefits derived from the treatment.

There are three possible responses to risk:

Risk Mitigation
Risk mitigation is the implementation of safeguards and countermeasures to reduce or eliminate vulnerabilities or threats.

Risk Transfer
Risk transfer is the placement of the cost of loss a risk represents onto another entity. This is accomplished by purchasing insurance and/or outsourcing.

Risk Acceptance
Acceptance of risk is the valuation by The AET that the cost/benefit analysis of a possible safeguard and the determination that the cost of the countermeasure greatly outweighs the possible cost of loss due to a risk. Values under 3 are acceptable risks, while values 3+ are unacceptable risks. Unacceptable risks must be treated. On behalf of the risk owners, Senior Management will accept all residual risks.

(5) Calculate Residual Risks

Based on risk treatment decisions, plans, and net new compensating controls to be implemented, residual risks must be calculated, reassessing the respective initial risks' likelihoods and impacts.

(6) Reporting

Roger Hanagriff or a designee is responsible for creating the risk assessment and treatment report and delivering results to senior management and other applicable personnel. This report shall include risk responses and documentation of risks that will be accepted by the organization such as threats or vulnerabilities that will likely impact the organization and with a low impact cost. All risk assessment reports must be documented and retained for a minimum of three years.

Unacceptable risks should be appropriately remediated or mitigated in accordance with the Change Management Policy and Vulnerability Management Policy.

Exceptions

The AET business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other The AET policy. If an exception is needed, The AET management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other The AET policy or procedure may result in disciplinary action, up to and including termination of employment. The AET reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. The AET does not consider conduct in violation of this policy to be within an employee’s or contractor’s course and scope of work.

Any personnel who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of The AET as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

Roger Hanagriff or a designee is responsible for overseeing the successful completion of the risk assessment. Such risk assessments must be conducted at least annually or whenever there are significant changes to The AET, its systems, or other conditions that may impact the security of The AET such as the failure of a mission critical vendor or a security breach.

The AET reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Roger Hanagriff.

This document was last updated on 01/29/2024.