THREAT AND RISK ASSESSMENT

HITACHI
Inspire the Next

A Threat and Risk Assessment (TRA) is a critical tool for understanding the various threats to your IT systems, determining the level of risk these systems are exposed to, and recommending the appropriate level of protection. If you are adding new applications or systems to your environment, making modifications to your existing Information Technology environment, or sharing information with new external entities, then you should perform a TRA on the new components to ensure that you are not introducing new risks. Periodic TRAs on existing environments are required, since the threat landscape continually changes and so do the vulnerabilities in your environment.

THREAT AND RISK ASSESSMENTS ARE DESIGNED TO:

- **Create the foundation of your organization's risk management program**
- **Ensure that appropriate measures are in place to protect confidentiality, integrity and availability of your corporate information**
- **Help you define your security risks and assess their relative magnitude**
- **Provide you with relevant information necessary to better manage risk**

WHAT IS A THREAT AND RISK ASSESSMENT?

A Threat and Risk Assessment provides analysis and interpretation of risks present in your organizational and technical environment. Hitachi Systems Security Inc. has in-depth knowledge and expertise in using security and IT control frameworks, such as the Harmonized TRA Framework, IT Infrastructure Library (ITIL), NIST, and the ISO 27000 series of IT security management best practices. The goal of a TRA is to provide you with relevant information necessary to make an informed decision as to how to best manage the identified risks.

SERVICE ELEMENTS

In conducting a Threat and Risk Assessment, Hitachi Systems Security Inc. uses the following approach:

- **Prepare and Plan –** The aim, scope, and boundaries of our system are defined; a system description is documented, and a concept of operation is defined.
- **Identify Assets & Assess Sensitivity –** Assets are identified and assessed according to confidentiality, integrity, and availability attributes.
- **Conduct Threat Analysis –** Threat agents are identified and scenarios are developed; capability, motivation, and likelihood are examined.
- **Conduct Vulnerability Analysis –** The types of attacks that system assets are vulnerable to are determined, and the level of effort (resources and capability) required by an agent to mount an attack is characterized.
- **Determine Residual Risks –** A measure of risk associated with the operation of your IT system is determined; risk is a function of the consequence of threat scenarios and the likelihood of their occurrence.
- **Prioritized Remediation Plan –** All identified risks are prioritized and a final overall assessment is provided to help form the basis of an overall effective risk mitigation strategy.

DELIVERABLES

Upon completion of a Threat and Risk Assessment, you will be provided with the following deliverables:

- Project Plan
- Threat and Risk Assessment—Includes work products from the phases:
  - Injury Table
  - System Description
  - Asset Valuation and Statement of Sensitivity
  - Control Review (Vulnerability) Assessment
  - Threat Assessment
  - Risk Assessment
  - Remediation Plans for treatment of the very high through medium priority risks
- Threat and Risk Assessment Presentation (if required)

OUTCOMES

- ✓ Identify and assign value to assets
- ✓ Identify vulnerabilities and associate them with the assets they expose
- ✓ Identify threats relevant to the vulnerabilities and assess them for likelihood and gravity
- ✓ Assess risk and prioritize recommendations for remediation