Risk Assessment for Information Resource

Standard ID
IOT-CS-SEC-100

Published Date
5/1/2006

Effective Date
5/1/2006

Last Updated
5/18/2017

Next Review Date
5/18/2018

Policy
04.0 Risk Assessment (ID.RA)
04.5 ID.RA-5
04.5.1 Risk Assessment

Purpose
Step one in sound risk management is a risk assessment. The practice identified below represents the State of Indiana’s minimum standard to be applied by State asset owners. This risk assessment process defined here is relatively simple. More sophisticated models are available and may be more appropriate for complex projects. Agencies or contracted resources having experience with other methodologies (e.g., NIST) are encouraged to apply them. Owners of information assets shall perform risk assessments prior to the implementation of the asset, upon discovery of new threats, and at regular intervals to assure currency.

Scope
IOT Supported Entities

Statement
Risk Assessment Procedure

- Each asset owner applies a risk-based approach to determine adequate security. Owners consider major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.
- Owners complete the risk assessment form using State templates (or one they or their contractors have as a standard).
- Risk assessment findings are documented that drive mitigating policy and practices.
- Agencies identify regularly scheduled monitoring and auditing activities as well as timeframes for re-assessment.
- Users and support personnel are made aware of risks and mitigation techniques.
- Monitoring for compliance with controls occurs regularly. Periodically, detailed objective audits are performed.
- Improvements identified from monitoring activities and audits are incorporated into plans to protect assets.

Information Technology Risk Assessment Process

Step 1 – Identify scope of the assessment and team member participation

The information asset owner is responsible for conducting risk assessments. The owner may lead the assessment or use a risk assessment facilitator. Assembling a capable team is critical. Business units and technical resources supporting system components are essential.

Step 2 – Gather information, evaluate threats and vulnerabilities
The team should consider risks, threats and vulnerabilities to the operation or asset assessed. The risk assessment form (Appendix A) lists vulnerabilities that are common or prominent (though they may not apply universally). Other vulnerabilities should be considered when they apply.

**Step 3 – Consider Possible Damage**

Teams should brainstorm scenarios that would result in damage. Damage possibilities include loss of public trust, monetary loss, loss of confidential citizen information, and system down time.

**Step 4 – Consideration of Controls**

Teams should consider the controls needed to protect against vulnerabilities described in Step 2 and prevent the damage described in Step 3. The controls in place may suffice, require modification, or additional controls may be needed to provide adequate security.

**Step 5 – Remaining Risk**

Teams will apply their judgment to determine if the remaining risk, after vulnerabilities, threats and controls are considered, is acceptable when compared to the business benefit.

The following guide may be helpful in determining the degree of risk. Damage possibilities can be projected by considering severity and probability.

**Severity**

- **Category 1** – Loss of confidential citizen information, compromise of public safety, extended system disruption, loss of an expensive asset, severe environmental damage, leaders and/or workforce viewed as incompetent.
- **Category 2** – Reduced level of public services, system disruption(s), significant assets damaged, environmental damage, State of Indiana performance stigma perpetuated
- **Category 3** – Minor, short term outages of service, assets impacted of minor value, minor environmental damage
- **Category 4** – Insignificant consequences to the citizenry, State assets, or the State workforce

**Probability**

- **Category A** – Frequent, potential for repeated incidents
- **Category B** – Probable, possibility of isolated incidents
- **Category C** – Occasional, possibility of eventual occurrence
- **Category D** – Remote, not likely to occur
- **Category E** – Improbably, likely not to happen

The chart below combines the factors above to assist with risk categorization.

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Probability of Occurrence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(A) Frequent</td>
</tr>
<tr>
<td>1 (High)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4 (Low)</td>
<td></td>
</tr>
</tbody>
</table>

Class 1 – (damage possibility must be addressed completely before proceeding)
Class 2 – (damage possibility requires corrective action, but some management discretion allowed)
Class 3 – (damage acceptable with review by management)
Class 4 – (damage acceptable without review)

**Step 6 – Additional controls and actions needed.**

**Roles**
Information Asset Owners/System Owners

**Responsibilities**
All new systems implemented must undergo a thorough risk assessment conducted by system owners. IOT Security/CISO will provide assistance and timely feedback to system owners as requested on their risk assessments.

**Management Commitment**
Management shall ensure that new systems undergo a proper risk assessment that meets the criteria defined in this standard.

**Coordination Among Organizational Entities**
Agencies shall coordinate with vendors and IOT as appropriate in conducting the risk assessment.

**Compliance**
Agencies shall provide assessments upon the request of IOT Security. For confidential systems that do not have an assessment completed, system owners shall plan and conduct a risk assessment within 6 months and demonstrate compliance with this standard.

**Exceptions**
Exceptions will be considered on a case by case basis by the CISO.