1.0 PURPOSE

This policy provides risk assessment requirements for Ohio Department of Administrative Services (DAS)-managed system assets. The requirements address preparing for, conducting, communicating and maintaining a risk assessment.

A glossary of terms found in this policy is located in Section 8.0 Definitions. The first occurrence of a defined term is in bold italics.

2.0 SCOPE

The scope of this policy includes any DAS-managed system assets.

This policy also applies to DAS data owners and service owners.

3.0 BACKGROUND

The risk assessment practice is designed to identify potential threats to system assets, associated impact, and the likelihood of the threat occurring. Risk assessments assist organizations in determining appropriate risk responses such as risk acceptance, risk avoidance, risk mitigation, risk sharing or risk transfer. Risk assessment outcomes can affect all aspects of the organization, such as 1) policy, procedure and guidance; 2) enterprise and security architecture decisions; and 3) design, implementation, and operations decisions.

4.0 REFERENCES

4.1 Ohio Administrative Policy IT-13, Data Classification: Ohio Administrative Policy IT-13 provides a data classification methodology to state agencies for the purpose of understanding and managing data and information systems with regard to their level of confidentiality and criticality.

4.2 Ohio IT Standard; ITS-SEC-02; Security Controls Framework: This state IT standard specifies the minimum requirements for information security in all agencies and identifies the National Institute of Standards and Technology (NIST)
Special Publication 800-53 (NIST 800-53) as the framework for information security controls implementation for the state.

4.3 **Federal Information Processing Standards (FIPS)-199**: FIPS-199 is the federal guideline for assessing and classifying information systems.


5.0 **POLICY**

*Data owners* and *service owners*, in coordination with the DAS Office of Information Security and Privacy (OISP), shall complete risk assessments on all existing DAS-managed system assets containing *sensitive IT system assets* and/or *business critical IT system assets*. In addition, risk assessments are required for any in-process or planned DAS-managed system asset development initiatives or procurements. Data owners and service owners shall also conduct risk assessments on any existing DAS-managed system assets, which if compromised or harmed, could potentially have a negative impact on the *confidentiality*, *integrity* or *availability* of information.

5.1 **Risk Assessment Methodology**: The National Institute of Standards & Technology (NIST) Special Publication (SP) 800-30, “Guide for Conducting Risk Assessments,” shall be used to assess risk for DAS-managed system assets. The NIST SP 800-30, “Risk Assessment Process,” illustrates the four core steps of the risk assessment methodology\(^1\). These steps shall be followed when conducting risk assessments on DAS-managed system assets. (Please refer to Figure 1 below for additional details.)

5.1.1 **Step 1: Prepare for Assessment**: Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

---

5.1.1.1 Identify the scope of the effort, which includes: time frame, organizational applicability, and the IT systems, resources and information that will be included in the risk assessment.

5.1.1.2 Define the assumptions and constraints associated with a given risk assessment (e.g., assumptions made regarding threat sources, vulnerabilities, likelihood, impacts, risk tolerance, approach).

5.1.1.3 Identify information sources for the threat, vulnerability and impact information.

5.1.1.4 Determine the risk model and analytic approach that will be used for the risk assessment.

5.1.1.4.1 It is recommended that DAS entities use the “Risk Master” tool designed by DAS OISP, which is aligned with NIST SP 800-30. The tool is available on the DAS.

---

5.1.2 **Step 2: Conduct Assessment**: The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to make informed risk response decisions.

5.1.2.1 Identify the *threat events* of concern;

5.1.2.2 Identify and characterize the most likely threat sources for the identified threat events, including capability, intent, and targeting characteristics for *adversarial threats* and the range of effects of non-adversarial threats;

5.1.2.3 Identify and document system vulnerabilities that could be exploited;

5.1.2.4 Analyze *security controls* that are already in place or are planned for implementation that minimize or eliminate the likelihood of a compromise occurring;

5.1.2.5 Determine the likelihood of potential vulnerabilities being exercised by a threat source;

5.1.2.6 Determine the impact associated with the compromise of DAS-managed system assets;

5.1.2.6.1 As part of the assessment process, *data classification labels* assigned in accordance with Ohio Administrative Policy IT-13, “Data Classification,” shall be closely reviewed to help determine the overall impact of a compromise of DAS-managed system assets.

5.1.2.7 Determine the level of risk using a rating methodology such as the one outlined in the DAS OISP developed “Risk Master” tool. As mentioned earlier, the tool is available on the DAS OISP Website at [InfoSec.ohio.gov](http://InfoSec.ohio.gov) within the “Resources” tab and under “IT Security Tools”.

5.1.2.8 Identify technical, operational and management controls that can mitigate or eliminate the identified risks; and

5.1.2.9 Document risk assessment results and control recommendations.
5.1.2.9.1 Control recommendations shall be based upon risk assessment results and shall align with the current version of NIST SP 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations,” as required in Ohio IT Standard ITS-SEC-02, “Enterprise Security Controls Framework.” The selection of individual controls shall be based upon system classification and an overall understanding of risks posed to DAS-managed system assets.

5.1.3 **Step 3: Communicate and Share Risk Assessment Results:** Communicate risk assessment results to organizational decision makers to support risk responses. In addition, share the results of the risk assessment with appropriate organizational personnel.

5.1.4 **Step 4: Maintain Assessment:** Conduct ongoing monitoring of the risk factors that could impact the risk to organizational operations and assets, individuals, or other organizations. Also, update existing risk assessments using the results from ongoing monitoring of risk factors (refer to section 5.3 for additional requirements regarding risk assessment updates).

5.2 **Risk Assessment Report:** The risk assessment results shall be documented in a risk assessment report and maintained by DAS OISP. The risk assessment report shall document the appropriate actions for managing identified risks. At a minimum, the following elements shall be included:

- **Treatment Action Items:** This is a list of suggested next steps and/or possible security controls that will help to lower the level of risk to DAS-managed system assets.

- **Due Dates:** The due date shall identify when action items are to be completed or security controls implemented.

- **Accountability:** The report shall identify a person responsible for ensuring that a treatment action item and/or security control is implemented.

5.2.1 The recommended DAS OISP “Risk Master” tool, when populated with the required data, will automatically generate a “Risk Assessment Report,” with input fields for documenting appropriate actions for managing identified risks.

5.3 **Risk Assessment Updates:** A new risk assessment shall be conducted every two years, or as a result of significant changes to a DAS-managed system asset’s environment or infrastructure, or following a significant security incident. A
significant change is defined as substantial changes that alter the mission, configuration or basic vulnerabilities of the DAS-managed system asset. Changes that may indicate the need for a new risk assessment include new or significantly changed:

- Business Requirements
- Hardware
- Application Programs
- External Users
- Telecommunications
- Location of the IT System (e.g., a new physical environment or a new organization)
- IT System Interfaces

6.0 PROCEDURES

None.

7.0 COMPLIANCE

As of the effective date of this policy, some DAS entities are unlikely to be completely aligned to the risk assessment requirements outlined in the policy. A general implementation framework for the requirements of this policy includes:

7.1 The risk assessment requirements for all existing DAS-managed system assets containing sensitive IT system assets and/or business critical IT system assets shall be implemented within six months from the effective date of the policy.

7.2 Any existing DAS-managed system assets, which if compromised or harmed, could potentially have a negative impact on the confidentiality, integrity or availability of information, shall comply with the risk assessment requirements outlined in this policy within one year of the effective date.

7.3 All planned and future DAS-managed system asset development initiatives or procurements, shall immediately comply with the risk assessment requirements outlined in this policy.

8.0 DEFINITIONS

Adversarial Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information,
and/or denial of service, conducted by an individual, group, organization, or government that has the intent to cause harm.

**Availability** - Ensuring timely and reliable access to and use of information. ³

**Business Critical IT System Assets** - Assets and/or systems that are identified as having the greatest potential to impact the achievement of the organizational mission.

**Confidentiality** - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. ⁴

**DAS-managed System Asset** - Information, hardware, software and services required to support state business, and identified during the risk assessment process as assets that need to be protected. Primary responsibility for managing these system assets may be assigned to DAS OIT personnel or other outside entities.

**Data Classification Labels** – Denotes the level of protection based on the confidentiality and criticality requirements of data in accordance with the agency’s risk assessment. Data classification labels enable policy-based standards for securing and handling data and sharing information among organizations. The terms, “data classification label” and “classification label,” are used interchangeably.⁵

**Data Owner** – In accordance with Ohio Administrative Policy IT-13, “Data Classification”, data owners shall be responsible for the identification and classification of information, in consultation with legal counsel. Data owners shall be responsible for the assignment of data classification labels, data compilation, data classification coordination and compliance, and data access as detailed in Ohio Administrative Policy IT-13.

**Integrity** - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. ⁶

**Risk** - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.⁷


⁴ Ibid.


⁷ Ibid.
**Risk Assessment** - The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.\(^8\)

**Risk Mitigation** - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.\(^9\)

**Security Controls** - Management, operational and technical policies, procedures and tools required to achieve and maintain the necessary level of assurance of confidentiality, integrity and availability.

**Sensitive IT System Assets** - Assets and/or systems that contain privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization.

**Service Owner** – A service owner is responsible for the delivery (design, performance, integration), continual improvement and management of assigned IT services.

**System Classification** - Refers to the process of assessing the potential impact to confidentiality, integrity and availability of the evaluated system. NIST SP 800-53 refers to Federal Information Processing Standards (FIPS)-199, which is the federal guideline for assessing and classifying information systems. DAS OISP plans to develop further guidance around system classification, but agencies can utilize the FIPS-199 publication until further guidance is released.

**Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.\(^10\)

**Threat Event** - A threat event is an event or situation initiated or caused by a threat source that has the potential for causing adverse impact.

**Threat Source** - The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.\(^11\)

---

\(^8\) Ibid.


\(^11\) Ibid.
**Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.\(^\text{12}\)

### 9.0 INQUIRIES

Direct inquiries about this policy to:

Office of Information Security & Privacy  
Office of Information Technology  
Ohio Department of Administrative Services  
30 East Broad Street, 19th Floor

1.614.644.9391 | state.isp@das.ohio.gov

DAS Policies may be found online at  
http://das.ohio.gov/Divisions/AdministrativeSupport/EmployeesServices/DASPolicies.aspx

Additional information regarding the Office of Information Security & Privacy may be found online at InfoSec.Ohio.Gov.

### 10.0 REVISION HISTORY

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/10/2017</td>
<td>Original Policy</td>
</tr>
<tr>
<td>04/10/2018</td>
<td>Scheduled policy review.</td>
</tr>
</tbody>
</table>

### 11.0 ATTACHMENTS

None.

---