

**Information Technology Risk Assessment (IT-RA)**

**Purpose:**

The purpose of an information technology risk assessment (IT-RA) is to provide the federal government, as well as senior leaders/executives and principal investigators, with the information needed to determine appropriate courses of action in response to identified risks. Risk assessments also help organizations monitor operations on an ongoing basis to determine whether risks have increased to unacceptable levels and have exceeded the organizations risk tolerance. As such, risk assessments should be conducted on an annual basis.

**Instructions:**

In accordance with the Information and Physical Access Security section of the contract, the contractor shall submit the IT-RA within thirty (30) days after contract award. The IT-RA shall be consistent, in form and content, with the latest revision of [NIST SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf), *Risk Management Guide for Information Technology Systems*, and any additions or augmentations described in the HHS-OCIO Information Systems Security and Privacy Policy. After resolution of any comments provided by the Government on the draft IT-RA, the Contracting Officer shall accept the IT-RA and incorporate the contractor’s final version into the contract for contractor implementation and maintenance. The contractor shall update the IT-RA on an annual basis.

**Please note:** The purpose, instructions and additional resource sections should not be included in the actual IT-RA form submitted to the Contracting Officer. These are references to aid the contract in completing its IT security contract deliverables. Please separate these sections and only submit the IT-RA form.

Before beginning an IT-RA, it is important to determine the scope of the assessment. The federal government understands that risk assessments can consume a significant amount of financial and personnel resources. As such, the scope of the risk assessment is left largely up to the contractor’s discretion. The scope of the assessment should be determined based on the overall security categorization for the system, the information system interconnections and sharing capabilities, and the resources available to the contractor.

For example, if the contractor will handle sensitive information such as personal health information or other identifiable information the scope of the risk assessment should encompass all the parameters outlined in this document and be comprehensive. If, however, confidentiality is not a concern, such as when personal health information is de-identified, the scope could potentially only touch upon elements that may impact availability and integrity as applicable. Contracts are encouraged to refer back to their FIPS 199 Assessment for determining the scope of the IT-RA. It should be noted that de-identification may require more than the removal of key PII data elements such as name and Social Security Number as other information about an individual when combined could provide identification e.g. describing a patient as having specific characteristics such as job, ethnicity etc. may not make them identifiable alone, but when combined with e.g. the name of the small town in which they live may make the information PII as it directly leads to a very small pool of possible individuals.

Once the scope of the assessment has been determined, the contractor is encouraged to review the latest revision of [NIST SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf), [*Guide for Conducting Risk Assessment*,](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)  to familiarize themselves with the risk assessment standards put forth by the National Institute of Standards and Technology (NIST). Additionally, the contractor is encouraged to look over the full list of Security Controls put forth in Table H-1: Mapping NIST SP 800-53 to ISO/IEC 27001 found in [NIST SP 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf), *Assessing Security and Privacy Controls for Federal Information Systems and Organizations*. Nonfederal information Systems and Organizations may find [NIST SP 800-171](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf), *Protecting Controlled Information in Nonfederal Information Systems and Organizations* may also be helpful. These resources are found under the Additional Resources section below.

This template should to be used as a guide. The types of threat sources, events and security controls have been derived from the [NIST 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf) and [NIST 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) documents and does not include the complete list of all threat sources, events or security controls identified by NIST but rather a selection based on the systems historically maintained by contractors. As such, some of the applicable threat sources, events, and security controls relevant to the contractor’s system may not be present and other events or controls may not apply. Examples of common threat sources and controls can be found below within the corresponding sections. Given the unique nature of biomedical research funded by the NHLBI using contracts, there will likely be additional areas of risk or threat that will need to be addressed.

This template has intentionally been left in .doc format to allow for modifications to fit the scope of the contractor’s system. Please modify the template to best fit the risk assessment being conducted.

The IT-RA should be signed by the contract Designated Approving Authority (DAA). The DAA is the individual who formally assumes responsibility for operating the information technology systems under the contract’s purview at an acceptable level of risk. The DAA is often the contractor’s Director of Information Technology, Chief Information Officer or similar role. The matrix and tables below will provide further instruction to aid the contractor in assessing security controls and measuring the associated risks with their system.

**Risk Matrix**

The risk matrix measures risks associated with threat sources, events and system security based on the likelihood of a vulnerability being exploited, the potential magnitude of impact, and the planned or existing security controls in place to eliminate or reduce risks.

**Type of Threat Source**

The types of threat sources listed below should be considered during a risk assessment to ensure adverse events are properly prepared for.

|  |  |
| --- | --- |
| **Type of Threat Source** | **Description**  |
| **ADVERSARIAL** * Individual
* Group
* Organizational
* Nation-State
 | Individuals, groups, organizations or states that seek to exploit the organization’s dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).  |
| **ACCIDENTAL** * User
* Privileged User/Administrator
 | Erroneous actions taken by individuals in the course of executing their everyday responsibilities.  |
| **STRUCTURAL** * IT Equipment
* Environmental Controls
* Software
 | Failure of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.  |
| **ENVIRONMENT** * Natural or man-made disaster
* Unusual Natural Event (e.g. sunspots)
* Infrastructure Failure/Outage
 | Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside of the control of the organization.  |

Examples of Threat Sources:

Adversarial Threat Source – Malicious groups intent on exploiting system vulnerabilities in an effort to gather PII to sell for profit on the black market.

Accidental Threat Source – Erroneous action taken by clinical trial investigator resulting in the loss of blinding in a trial and compromising study integrity.

Structural Threat Source – Applications no longer supported by vendor could leave systems vulnerability to security vulnerabilities that the vendor will no longer be supplying patches for.

 Environment – Servers stored within a location prone to flooding and high winds from coastal storms could lead to power outages resulting in server downtime and loss of data.

More information on the types of threat sources can be found in NIST publication 800-30 Table D-2: Taxonomy of Threat Sources.

**Likelihood Determination**

The likelihood of an event or vulnerability occurring should be considered when calculating the risk of a system. Some factors to consider:

* Threat source motivation and capability
* Nature of the vulnerability
* Existence and effectiveness of current controls.

|  |  |
| --- | --- |
| **Level** | **Likelihood Definition** |
| **High** | The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.  |
| **Moderate** | The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability |
| **Low** | The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.  |

Example of Likelihood Determination:

The threat source is motivated and capable of exploiting system vulnerabilities through a phishing email attack however controls such as a Barracuda spam firewall, baseline workstation configuration, policies and procedures on storing, sharing and accessing sensitive information and security awareness training are in place that may impede the successful exercise of this vulnerability. Therefore an adversarial threat source, such as malicious phishing attack, has a likelihood determination of **Moderate**.

**Impact Analysis**

Measuring level of risk should be determined by the adverse impact resulting from successful exploitation of a vulnerability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals:

* Loss of Confidentiality – Impact of unauthorized disclosure of sensitive information
* Loss of Integrity – Impact if system or data integrity is lost by unauthorized changes to the data or systems.
* Loss of Availability – Impact of system functionality and operational effectiveness

|  |  |
| --- | --- |
| **Magnitude of Impact** | **Impact Definition** |
| **High** | Exercise of the vulnerability - may result in the highly costly loss of major tangible assets or resources; may significantly violate, harm, or impede an organizations mission, reputation, or interest, or; may result in human death or serious injury.  |
| **Moderate** | Exercise of the vulnerability – may result in the costly loss of tangible assets or resources; may harm or impede an organization’s mission, reputation, or interest; or may result in human injury. |
| **Low** | Exercise of the vulnerability – may result in the loss of some tangible assets or resources; may noticeably affect an organization’s mission, reputation, or interest.  |

Example of Impact Analysis:

The impact of a successfully executed phishing attack would likely result in the loss of some resources such as proprietary research which may noticeably affect an organization’s mission, reputation or interest. However, since personally identifiable information is de-identified and not stored locally on workstations there would not be any harm to an organization’s mission, reputation or interest should such an event occur. Therefore the impact would be **Low**.

**Risk Determination**

The following factors should be used to assess the level of risk to the system:

* The likelihood of a given threat source’s attempting to exercise a given vulnerability
* The magnitude of the impact should a threat-source successfully exercise the vulnerability
* The adequacy of planned or existing security controls for reducing or eliminating risk

|  |  |
| --- | --- |
| **Magnitude of Impact** | **Risk Level Definition** |
| **High** | There is a strong need for corrective measures. An existing system may continue to operate but a corrective action plan must be put in place as soon as possible.  |
| **Moderate** | Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.  |
| **Low** | The system’s Designated Approving Authority must determine whether corrective actions are still required or decide to accept the risk.  |

Example of Risk Determination:

The likelihood of a phishing attack to occur is **Moderate** however the impact of a successful exploit would be **Low**. Therefore the Risk Level Determination is **Low** and the Designated Approving Authority has opted to accept this risk rather than take corrective action.

**Additional Resources:**

[Guide for Conducting Risk Assessment NIST SP 800-30](http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf)

[Security and Privacy Controls for Federal Information Systems and Organizations NIST SP 800-53](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

[Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations NIST SP 800-171](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf)

## Name of Organization

## Name of System

## Information Technology Assessment (IT-RA)

## Insert version

Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Approval Date: \_\_\_\_\_\_\_\_\_\_

 Insert Approver Title

Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Approval Date: \_\_\_\_\_\_\_\_\_\_

 Insert Approver Title

Approved By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Approval Date: \_\_\_\_\_\_\_\_\_\_

 Insert Approver Title

This is an INSERT NAME OF ORGANIZATION internal document. It shall be used and disclosed externally for evaluation purposes only. Disclosure of this document outside the Government for any purpose is strictly forbidden.

# **Document Revision History**

| Date | Author | Version | Change Reference |
| --- | --- | --- | --- |
|  |  |  |  |
| 00/00/0000 |  | 1.0 | Drafted document |

|  |
| --- |
| **Contract Overview** |
| Project Title |
| Contract/Solicitation Number |
| Contracting Officer |
| Contract Awardee | Award Date |
| **System Overview** |
| System Name |
| System Description  |
| System Interconnections/Information Sharing |
| **Overall System Security Category** *(Reference FIPS-199 Assessment)* |
| [ ]  Low [ ]  Moderate [ ]  High |
| **Overall Impact Levels***(Reference FIPS-199 Assessment)* |
| ConfidentialityChoose an item. | IntegrityChoose an item. | AvailabilityChoose an item. |
| **Threat Sources and Events Assessment** *(Reference NIST 800-30)* |
| *Example of a Threat Source and Event Assessment* |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *Environmental* | *The data center which houses the web and database servers is in an area prone to ice storms in the winter which can bring down power lines causing wide spread power outages.*  | *CP-9 (Information System Backup) – servers are backed up daily to prevent data loss should power outage cause any loss of data.* *CP-2 (Contingency Plan) – is in place to allow data collection to occur locally on workstations until the data center comes back online.*  | *Moderate* | *Low* | *Low*  |
| *Comments* *to Control(s):*  | *CP-6 (Alternate Storage Site) - We are planning to acquire storage at an alternate data center site which could come online and take over operations should the power go out in the existing data center housing the web and database servers. This is planned to be implemented in fiscal year 2017.*  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments to Control(s):  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments to Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments to Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
|  |  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **System Vulnerabilities Assessment** *(Reference Table H-1 NIST SP 800-53 Controls from NIST 800-53 document or NIST 800-171 if more applicable and IT-SP)* |
| *Example of System Vulnerabilities Assessment* |
| *Type* | *Description* | *Security Controls In Place*  | *Likelihood* | *Magnitude of Impact* | *Risk Level*  |
| *AC-11* | *Session Lock*  | *Workstations are set to lock sessions automatically after 15 minutes of inactivity.* *Web server does not presently have this feature enabled.*  | *Low* | *Low* | *Low* |
| *Comments on Control(s):* | *We plan to enable automatic session locks when we upgrade the web server next year. However the risk is low since standard users do not have the ability to access sensitive or protected information. No corrective action is required at this time.*  |
| **Access Control (AC)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-1* | Access Control Policy and Procedures |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-2* | *Account Management*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-3* | *Access Enforcement*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-4* | *Information Flow Enforcement*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-5* | *Separation of Duties*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-6* | *Least Privilege* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-7* | *Unsuccessful Logon Attempts*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-8* | *System Use Notification*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-11* | *Session Lock*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-12* | *Session Termination*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-14* | *Permitted Actions without Identification or Authentication*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-17* | *Remote Access*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-18* | *Wireless Access* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-19* | *Access Control for Mobile Devices*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-20* | *Use of External Information Systems*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-21* | *Information Sharing*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AC-22* | *Publicly Accessible Content*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| **Awareness & Training (AT)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AT-1* | *Security Awareness and Training Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AT-2* | *Security Awareness Training*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AT-3* | *Role-Based Security Training*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Audit and Accountability (AU)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AU-1* | *Audit and Accountability Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AU-2* | *Audit Events*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AU-4* | *Audit Storage Capacity* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AU-6* | *Audit Review, Analysis, and Reporting*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AU-8* | *Time Stamps*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *AU-11* | *Audit Record Retention*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Security Assessment and Authorization (CA)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *CA-3* | *System Interconnections*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Configuration Management (CM)**  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *CM-2* | *Baseline Configuration* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *CM-5* | *Access Restrictions for Change*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| CM-7 | *Least Functionality*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Contingency Planning (CP)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| CP-1 | *Contingency Planning Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| CP-2 | *Contingency Plan*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| CP-3 | *Contingency Training*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *CP-6* | *Alternative Storage Site*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *CP-9* | *Information System Backup*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *CP-10* | *Information System Recovery and Reconstitution*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |  |  |  |  |
| **Identification & Authentication (IA)**  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *IA-1* | *Identification and Authentication Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *IA-2* | *Identification and Authentication*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Incident Response (IR)**  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *IR-1* | *Incident Response Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *IR-6* | *Incident Reporting*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *IR-8* | *Incident Response Plan*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Maintenance (MA)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MA-1* | *System Maintenance Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MA-3* | *Maintenance Tools*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MA-6* | *Timely Maintenance*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Media Protection (MP)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MP-1* | *Media Protection Policy and Procedures*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MP-4* | *Media Storage*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MP-6* | *Media Sanitization*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *MP-7* | *Media Use*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Physical & Environmental Protection (PE)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| PE-3 | Physical Access Control |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-4* | Access Control for Transmission Medium  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-5* | *Access Control for Output Devices* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-6* | *Monitoring Physical Access* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level*** |
| *PE-8* | *Visitor Access Records*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-9* | *Power Equipment and Cabling*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-10* | *Emergency Power*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-13* | *Fire Protection*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-14* | *Temperature and Humidity Controls* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-15* | *Water Damage Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PE-17* | *Alternate Work Site* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Planning (PL)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PL-4* | *Rules of Behavior*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Personnel Security (PS)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PS-3* | *Personnel Screening*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PS-4* | *Personnel Termination*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PS-6* | *Access Agreements*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *PS-7* | *Third Party Personnel Security* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Risk Assessment (RA)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *RA-5* | *Vulnerability Scanning*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **System & Communications Protection (SC)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-5* | *Denial of Service Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-7* | *Boundary Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-8* | *Transmission Confidentiality and Integrity* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-10* | *Network Disconnect* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-13* | *Cryptographic Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-15* | *Collaborative Computing Devices* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-17* | *Public Key Infrastructure Certificates*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-23*  | *Session Authenticity* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-28* | *Protection of Information at Rest*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SC-39* | *Process Isolation* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **System & Information Integrity (SI)** |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| *SI-3* | *Malicious Code Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| SI-5 | *Security Alerts, Advisories, and Directives*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| SI-8 | *Spam Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| SI-10 | *Information Input Validation*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| SI-11 | *Error Handling*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| SI-12 | *Information Handling and Retention*  |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| ***Type*** | ***Description*** | ***Security Controls In Place***  | ***Likelihood*** | ***Magnitude of Impact*** | ***Risk Level***  |
| SI-16 | *Memory Protection* |  | Choose an item. | Choose an item. | Choose an item. |
| Comments on Control(s): |  |
| **Overall System Risk Determination**Based on the Threat Sources, Events and System Vulnerabilities Assessment completed above, the system’s overall risk is defined as:  |
| [x]  Low [ ]  Moderate [ ]  High |
| Justification of Overall System Risk Determination: |  |
| **Risk Assessment Performed by:**  |
| Name | Organization | Title  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| **Designated Approving Authority** |
| Name: | Title: |
| Address: |
| Phone: | Email:  |
| *By signing below, the DAA acknowledges they have reviewed the IT Risk Assessment in its entirety and accepts responsibility for operating the information technology systems under the contract’s purview at the identified level of risk.*  *\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* *DAA Signature DAA Title Date* |