INSTRUCTIONS FOR RISK ACCEPTANCE FORM

This form is to be used to justify and validate a formal Risk Acceptance of a known deficiency. The system's business owner is responsible for writing the justification and the compensating control or remediation plan. It is a requirement that a compensating control or remediation plan be defined in order to obtain full approval for a Risk Acceptance.

The items below must be completed by the affected Department:

1) **IDENTIFY THE ORIGIN OF THE DEFICIENCY, VULNERABILITY, EXCEPTION**
   Check the appropriate Assessment, Audit, Policy, Service, Standard, System, or other item as applicable.

2) **RISK RATING**
   Assess and rate the overall risk presented in this document and assign a risk score. **If there are questions on the risk score, please review the Addendum in the back of the form**.

3) **LIST THE DEFICIENCY, VULNERABILITY, EXCEPTION**
   Apply the appropriate National Institute of Standards and Technology (NIST) control deficiency or vulnerability and/or other identified risk factor.

4) **DESCRIPTION OF DEFICIENCY, VULNERABILITY, EXCEPTION**
   Provide an overall summary of the deficiency or vulnerability. The summary is a description derived from the review of the appropriate Application, Arizona Baseline Control submission, Assessment, Audit, Policy, Service, Standard, System, or other item as applicable, in order to provide formal validation. Be as specific and detailed as possible.

5) **JUSTIFICATION FOR RISK ACCEPTANCE**
   Justify requesting a Risk Acceptance versus remediating the deficiency(ies).

6) **DESCRIBE THE COMPENSATING CONTROL OR REMEDIATION PLAN**
   In order to obtain a Risk Acceptance for a deficiency, a compensating control or remediation plan must be put in place and documented. A very detailed description must be provided in writing, and the approving individuals must acknowledge accepting the compensating control or remediation plan.

7) **ADDITIONAL REMARKS**
   Provide any other comments and supporting material required for the Risk Acceptance.

8) **ACKNOWLEDGEMENT AND APPROVALS**
   In order for the Risk Acceptance to be submitted to ADOA/ASET Security Office, obtain the necessary signatures as indicated below:

   a. **Division Director**: Required. To sign off indicates that they understand and accept the risk of a deficiency(ies) versus remediating the deficiency on behalf of the division.

   b. **Agency Chief Information Officer**: Required. To sign off indicates that they accept and understand that the Division in their agency has accepted risk of a deficiency(ies) versus remediation.

   c. **Agency Director**: To sign off indicates that they accept and understand that the Department/Division, Board or Commission has accepted risk of a deficiency(ies) versus remediating the deficiency.

   d. **State Chief Information Security Officer & State Chief Information Officer**: Required. To sign off Indicates that they acknowledge or accept and understand that the Department/ Division, Board or Commission has accepted risk of a deficiency(ies) versus remediating the deficiency.

   NOTE: Any risk acceptance requested for systems containing data classified as CONFIDENTIAL (PII, PHI, etc.) REQUIRE the State CIO or their designee to sign.

ARIZONA DEPARTMENT OF ADMINISTRATION ARIZONA STRATEGIC ENTERPRISE TECHNOLOGY	**RISK ACCEPTANCE FORM**
This form is to be used to document, justify and formally accept risk for a known deficiency(ies). The agency/division is responsible for writing the justification and identifying the compensating control.	

1. IDENTIFY THE ORIGIN OF THE DEFICIENCY, VULNERABILITY OR EXCEPTION - CHECK ONE BOX (**COMPLETED BY AGENCY)**

☐	Application	☐	Service
☐	Assessment	☐	Standard(s)
☐	Audit	☐	System
☐	Baseline Control	☐	Other*
☐	Policy(ies)		

*explain in detail

---

2. RATE THE OVERALL RISK SCORE OF THE DEFICIENCY, VULNERABILITY OR EXCEPTION - SELECT ONE RISK LEVEL AND ASSIGN A VALUE IN THE SELECTED BOX* (**COMPLETED BY AGENCY)**

High ☐ Moderate ☐ Low ☐

*The overall risk score will be calculated using the Business Risk Determination Questionnaire found at aset.az.gov/resources/policies-standards-and-procedures. The addendum attached to this form may also be used.

The following items must be completed (include as much detail as possible):

3. LIST THE IDENTIFIED DEFICIENCY, VULNERABILITY OR EXCEPTION (**COMPLETED BY AGENCY)**

4. DESCRIPTION OF THE DEFICIENCY, VULNERABILITY OR EXCEPTION **(COMPLETED BY AGENCY)**

5. JUSTIFICATION FOR RISK ACCEPTANCE **(COMPLETED BY AGENCY)**

6. DESCRIPTION OF THE COMPENSATING CONTROL OR REMEDIATION PLAN TO BE PUT IN PLACE TO REPLACE OR CORRECT THE DEFICIENCY, VULNERABILITY OR EXCEPTION (**COMPLETED BY AGENCY)**

7. ADDITIONAL REMARKS (**COMPLETED BY DIVISION/AGENCY)**

8. ACKNOWLEDGEMENT AND APPROVALS

STATEMENT OF UNDERSTANDING

RISK HAS BEEN ACCEPTED BY THE AGENCY OR DIVISION (**COMPLETED BY DIVISION/AGENCY CIO & AGENCY DIRECTOR)**

We acknowledge and understand that a division in our department(s) has/have accepted responsibility for the identified outstanding risk(s) and all subsequent impact(s) related to the deployment and use of this Application, Assessment, Audit, Policy, Service, Standard or System (or other item as applicable) for the period of no more than three (3) calendar years from date of approval with risk acceptance notifications at least annually. We find the controls that have been addressed in this document are adequate, and additional controls need not be applied. We also understand that this exception may be revoked by the State's Chief Information Officer (CIO) or designee at any time and may be subject to any annual follow-up procedures by internal audit.

APPROVAL SIGNATORIES

○ Accept ○ Deny

Division Director *(sign above line)* | Print Name | Email Address | Date

○ Accept ○ Deny

Department Information Security Officer *(sign above line)* | Print Name | Email Address | Date

○ Accept ○ Deny

Department Chief Information Officer *(sign above line)* | Print Name | Email Address | Date

○ Accept ○ Deny

Department Director *(sign above line)* | Print Name | Email Address | Date

○ Accept ○ Deny ○ Acknowledge

State Chief Information Security Officer *(sign above line)* | Print Name | Email Address | Date

○ Accept ○ Deny ○ Acknowledge

State Chief Information Officer *(sign above line)* | Print Name | Email Address | Date

Monthly

Risk Acceptance Notification Frequency | Risk Acceptance End Date

Important: *Notification Frequency must occur at least annually to all signatories.*

Risk Acceptance End Date shall not exceed three years from Risk Acceptance approval.

ADDENDUM: Risk factors and Determination of Risk Methodology

Business Risk Determination Questionnaire

https://aset.az.gov/resources/policies-standards-and-procedures

(Practical Risk Measurement Guidelines based on OWASP)

The likelihood of a security incident occurrence is a function of the likelihood that a threat appears and the likelihood that the threat can successfully exploit the relevant system vulnerabilities.

The consequence of the occurrence of a security incident is a function of likely impact that the incident will have on the organization as a result of the harm the organization assets will sustain. Harm is related to the value of the assets to the organization; the same asset can have different values to different organizations.

So R can be function of four factors:

- A = value of the assets
- T = the likelihood of the threat
- V = the nature of vulnerability i.e. the likelihood that can be exploited (proportional to the potential benefit for the attacker and inversely proportional to the cost of exploitation)
- I = the likely impact, the extent of the harm

- **FACTORS INVOLVED IN CALCULATING LIKELIHOOD**:
  - Threat agent factors
    - Skill level: How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (4), network and programming skills (6), security penetration skills (9)
    - Motive: How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
    - Opportunity: What resources and opportunity are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
    - Size: How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)
  - Vulnerability Factors: the next set of factors is related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.
    - Ease of discovery: How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
    - Ease of exploit: How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
    - Awareness: How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
    - Intrusion detection: How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

- **FACTORS INVOLVED IN CALCULATING IMPACT**

    - **Technical Impact Factors;** technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.
        - **Loss of confidentiality**: How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
        - **Loss of integrity**: How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
        - **Loss of availability** How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
        - **Loss of accountability:** Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

    - **Business Impact Factors:** The business impact stems from the technical impact, but requires a deep understanding of what is important to the company running the application. In general, you should be aiming to support your risks with business impact, particularly if your audience is executive level. The business risk is what justifies investment in fixing security problems.
        - **Financial damage:** How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
        - **Reputation damage:** Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
        - **Non-compliance:** How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
        - **Privacy violation:** How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)