pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Risk Assessment and Acknowledgment

Number OPD-SEC040A	**Effective Date** July 18, 2018
Category Security	**Supersedes** OPD-BUS011A
Contact RA-ITCentral@pa.gov	**Scheduled Review** July 2024

This point-in-time Risk Assessment and Acknowledgement document records that Agency Business Owners have been notified of, understand, and acknowledge the risk(s) associated with procuring or implementing this business and technology solution or service. This form may be used for solutions that are hosted or provided by the Commonwealth or external Service Organizations (per criteria as set forth in RFD-BUS004B).

Agency Business Owners (3):

- Agency Deputy Secretary for Administration or Agency Secretary
    - Always required to sign. The Agency Deputy Secretary by signing is certifying that they understand and acknowledge the risk(s) as outlined within this form and that in the event an issue occurs, they will acknowledge responsibility for the risk(s) that were outlined within this form.
- Agency Business Area Contact (Bureau Director)
    - Always required to sign. The Bureau Director by signing is certifying that they understand and acknowledge the risk(s) as outlined within this form and that in the event an issue occurs, they will acknowledge responsibility for the risk(s) that were outlined within this form.
- Agency Office of Chief Counsel (Agency Legal Counsel)
    - Always required to sign. The Agency Legal Counsel by signing certifies that they have been consulted in connection with the risks and waiver requests outlined within this form and that they have advised the agency and delivery center of the potential legal concerns associated with the waiver and risks identified.

Section 1: Risk Assessment (Risk Identification and Recommendation)

Part I - V is to be completed by the **Delivery Center or Agency Information Security Officer (ISO)** to document policy non-compliance and associated risk. Information is to be used by Agency Business Owners to make well informed decisions about risk.

Section 2: Risk Acknowledgement

Part VI - VII is to be completed and signed by the **Agency Business Owners** to acknowledge the risk(s) associated with the business and technology solution or service.

Section 1: Risk Assessment

Part I - Summary (Identify the asset, Threat Community, vector, and impact)
(Risk Exposure = Impact * Probability)

- High – Will probably occur in most circumstances without Compensating Controls
- Moderate – Might occur at some time without Compensating Controls
- Low – Could occur at some time without Compensating Controls

Name of Business Solution or Service	
Affected Organization	
Use Case Title (SR#xxxxx)	
Enterprise Application Inventory ID (AgencyID-999)	
Application Delivery Services	
Business Criticality	
COOP Tier	
Asset(s):	
Most Restrictive Data (Refer to ITP-INF015)	

Risk ID Refer to Table 1	Risk Summary	Risk Owner	Inherent Risk	Residual Risk	Risk Recommendation	Target Remediation

Part II - Risk Description (see Table 1 Risk ID and Categories at end of form)

(Risk Exposure = Impact * Probability)

- High – Will probably occur in most circumstances with Compensating Controls
- Moderate – Might occur at some time with Compensating Controls
- Low – Could occur at some time with Compensating Controls

Risk ID Refer to Table 1	Finding	Inherent Risk	Compensating Controls	Residual Risk	Consequence	Corrective Action	Remediation Timeframe

Part III - Risk Description (see Table 1 Risk ID and Categories at end of form)
(Risk Exposure = Impact * Probability)

- High – Will probably occur in most circumstances with Compensating Controls
- Moderate – Might occur at some time with Compensating Controls
- Low – Could occur at some time with Compensating Controls

Risk ID Refer to Table 1	Probability of Occurrence Enter High, Moderate, or Low	Risk Owner	Rationale/Risk Description Provide detailed narrative of why the risk rating has been selected.

Part IV - Action Plan Milestones (reference Part II Controls)

#	Milestone Description	Contact	Artifact	Indicate if control is Required or Recommended to proceed
1				
2				
3				
4				
5				
6				

Part V - ISO Attestation (Based upon the information provided and/or available at the time of review, potential risks have been identified and the business has been informed of the risks in Parts I-IV)

Delivery Center or Agency ISO	<Insert Name – Required>	<MM/DD/YYYY>

Section 2: Risk Acknowledgement

Part VI - Risk to Business (Risk Appetite/Risk Exposure)		
Risk Category	Risk Question	Response
Financial Damage	What is the potential financial impact due to fines, punitive damages, loss of revenue, or judgments resulting from a service disruption, data manipulation, data exposure, etc.? 1. Low <$100k 2. Medium $100k-$1million 3. High $1 million +	
Non-Compliance	How much risk will result due to non-compliance (ITP, Management Directives, Regulatory requirements)? 1. Minor / Moderate finding 2. Major finding 3. Fines against the agency 4. Loss of federal access/data/grants	
Reputation Damage	Would a service disruption, data manipulation, data exposure, etc. result in reputation damage that would harm the business? 1. None 2. Minor damage 3. Moderate damage 4. Major damage	
Privacy Violation	How many closed records, e.g., personally identifiable information could be disclosed? 1. Less than 100 records 2. Hundreds of records 3. Thousands of records 4. Millions of records	

Health, Safety, Welfare	Would a service disruption or data exposure result in negatively impacting the health, safety, or welfare of commonwealth citizens or employees? 1. Less than 100 records 2. Hundreds of records 3. Thousands of records 4. Millions of records	
Operational Risk	Would a service disruption result in a degree of disruption of business operations? 1. Secondary operations interrupted 2. Minimal or temporary interruption to essential operations 3. Extensive interruption to secondary operations 4. Extensive essential operations interrupted 5. Essential and secondary operations interrupted	

Part VII – Approvals (Acknowledgement is required from all parties)		
Agency Deputy Secretary for Administration or Agency Secretary	<Insert Name – Required>	<MM/DD/YYYY>
Agency Business Area Contact (Bureau Director)	<Insert Name - Required>	<MM/DD/YYYY>
Agency Office of Chief Counsel	<Insert Name - Required>	<MM/DD/YYYY>

Table 1 – Risk IDs

Table 1 Risk IDs – **ITP-SEC040** Cloud Services Requirements (CSRs) / All other relevant ITPs / NIST Controls / Legal Terms	
CSR-L1	Procurement Requirement
CSR-L3	CONUS Access Control
CSR-L4	CONUS Hosting
CSR-L5	System and Organization Controls (SOC) Reporting. Include risk related to any exceptions or findings from SOC Reports.
CSR-A1	Accessibility Standards
CSR-IN1	System Design Review of Electronic Information Systems Questionnaire
CSR-S1	System Monitoring / Audit Logging (Security)
CSR-S2	Boundary Protection / Network Protection
CSR-S3	Exploit and Malware Protection
CSR-S4	Encryption
CSR-S5	Identity & Access Management
CSR-S6	Vulnerability Assessment
CSR-S7	Service Availability / Recovery
CSR-S8	Compliance (all federal and state statues, laws, and policies)
CSR-S9	Security Incident Handling
CSR-S10	Inventory
CSR-I1	Connectivity
CSR-I2	Interface Requirements
CSR-I3	System Monitoring / Audit logging (Infrastructure)
CSR-I4	Capacity
Applicable ITPs	List applicable ITP Number as the Risk ID (e.g., SEC019, SEC007, SEC031, etc.).

NIST publication IDs	List applicable NIST 800-53 Control Family(ies) (e.g., NIST 800-53 R4 CA-1)
Legal Terms **(Indicate 1, 2, 3, and/or 4)**	Any terms and conditions accepted by the Agency must be approved as to form and legality (approved by Agency, Agency Counsel, Office of General Counsel, Office of Attorney General, and, if applicable, Office of Comptroller Operations). 1 - IT Terms and Conditions 2 - Software License Agreement 3 – Requirements for Non-Commonwealth Hosted Applications/Services 4 - Vendor’s EULA/Agreement

INSTRUCTIONS

Section 1: Risk Assessment

Part I - Summary (Identify the asset, Threat Community, vector, and impact)
(Risk Exposure = Impact * Probability)

High – Will probably occur in most circumstances without Compensating Controls
Moderate – Might occur at some time without Compensating Controls
Low – Could occur at some time without Compensating Controls

Name of Business Solution or Service	*The common name of the business solution or service. Should not contain any acronyms or agency jargon. Name should be the exact same as it is in Enterprise Application Inventory or other official publication.*
Affected Organization	*Affected Organization - Enter the line of business name or Enterprise if the entire Commonwealth is at risk.*
If cloud-based service, Cloud Use Case Title	*(SR# and Use Case Title)*
Enterprise Application Inventory ID (AgencyID-999)	*This is used to link a risk assessment to the captured information about the solution in Enterprise Application Inventory. Application inventory must be up to date and provide a clear understanding of the application, its purpose, and the technology.*
Application Delivery Services	*Consider if Application/Service is a resource that enables and/or provides the delivery of services(s):* *Choose one of the following:* • *Primary – Mission Critical/Business Essential* • *Secondary – Business Core/Supporting*
Business Criticality	*Is this application/solution associated with or linked to a Mission Critical Function in your agency's COOP plan?* *(Yes / No)*
COOP Tier	*If this application/solution is tied to a Mission Critical function (i.e., is Business Essential) what is the length of disruption the agency can sustain before measurable impact is realized to business capability, citizens (health/life/safety), Financial Losses or Liabilities, and Reputation.* • *Tier I – Application or Service is needed to support a business function, can only sustain a ONE DAY Disruption* • *Tier II – Application or Service is needed to support a business function, can sustain up to a ONE WEEK Disruption* • *Tier III – Application or Service is needed to support a business function, can sustain up to a*

	ONE MONTH Disruption
Asset(s):	*The thing(s) we're trying to protect (people, data, business services, infrastructure, etc.)*
Most Restrictive Data (refer to ITP-INF015)	*Data Classification per ITP-INF015*

Risk ID Refer to Table 1	Risk Summary	Risk Owner	Inherent Risk	Residual Risk	Risk Recommendation	Target Remediation
Risk ID from Table 1	*Specific risk scenario 1*	*A person, not office or resource account*	*From Risk Register or this Assessment – High, Moderate, or Low*	*The risk that remains after a compensating control or mitigation is applied.*		*Pre Go-Live, or Post Go- live*
Risk ID from Table 1	*Specific risk scenario 2*	*A person, not office or resource account*	*From Risk Register or this Assessment – High, Moderate, or Low*	*The risk that remains after a compensating control or mitigation is applied.*		*Pre Go-Live, or Post Go- live*

Part II - Risk Description (see Table 1 Risk ID and Categories at end of form)
(Risk Exposure = Impact * Probability)

High – Will probably occur in most circumstances with Compensating Controls
Moderate – Might occur at some time with Compensating Controls
Low – Could occur at some time with Compensating Controls

Risk ID Refer to Table 1	Finding	Inherent Risk	Compensating Controls	Residual Risk	Consequence	Corrective Action	Remediation Timeframe
Risk ID from Table 1	*The deviation from the requirements of Commonwealth IT Policy, standards or guidelines, law, regulation, or best practice.*	*Inherent risk is current or initial risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls.*	*What safeguard or countermeasure should be in place to mitigate the risk?* *What safeguards are in place to help reduce the risk of the issue?*	*What level of risk remains after compensating controls are implemented – High, Moderate, or Low?*	*What can happen; noncompliance, litigation, financial, breach of contract, data compromise, etc.*	*Description of remediation efforts and parties involved*	*e.g., before procurement, Pre-Go-live, within first year, etc.*
Risk ID from Table 1	*The deviation from the requirements of Commonwealth IT Policy, standards or guidelines, law, regulation, or best practice.*	*Inherent risk is current or initial risk level given the existing set of controls rather than the hypothetical notion of an absence of any controls.*	*What safeguard or countermeasure should be in place to mitigate the risk?* *What safeguards are in place to help reduce the risk of the issue?*	*What level of risk remains after compensating controls are implemented – High, Moderate, or Low?*	*What can happen; noncompliance, litigation, financial, breach of contract, data compromise, etc.*	*Description of remediation efforts and parties involved*	*e.g., before procurement, Pre Go-live, within first year, etc.*

Part III - Risk Description (see Table 1 Risk ID and Categories at end of form)

(Risk Exposure = Impact * Probability)

High – Will probably occur in most circumstances with Compensating Controls
Moderate – Might occur at some time with Compensating Controls
Low – Could occur at some time with Compensating Controls

Risk ID Refer to Table 1	Probability of Occurrence Enter High, Moderate, or Low	Risk Owner	Rationale/Risk Description Provide detailed narrative of why the risk rating has been selected.
Risk ID from Table 1	*High, Moderate, or Low*		*Estimate probability, include assumptions, rationale, threat community motives, etc. Calibrate the estimate*
Risk ID from Table 1	*High, Moderate, or Low*		*Estimate probability, include assumptions, rationale, threat community motives, etc. Calibrate the estimate*

Part IV - Action Plan Milestones (reference Part II Controls**)**

#	**Risk ID** Refer to Table 1	Milestone Description	Contact	Artifact	Indicate if control is Required or Recommended to proceed
1	*Risk ID from Table 1*	Example: Design a solution to the issue	*A person, not office or resource account*	e.g., solution design document, or controls documentation	*Required or Recommended to proceed*
2	*Risk ID from Table 1*	Example: Design a solution to the issue	*A person, not office or resource account*	e.g., solution design document, or controls documentation	*Required or Recommended to proceed*

Section 2: Risk Acknowledgement

Part VI – Risk to Business

Business leaders need to understand the risk. Use the table, questions, and considerations above to respond in Part VI above.

Part VI - Risk to Business (Risk Appetite/Risk Exposure)		
Risk Category	**Risk Question**	**Response**
Financial Damage	What is the potential financial impact due to fines, punitive damages, loss of revenue, or judgments resulting from a service disruption, data manipulation, data exposure, etc.? 1. Low <$100k 2. Medium $100k-$1million 3. High $1 million +	*Consider the number of records. Engage OCC to determine if citizens have sued the Commonwealth/agency in the past. Will federal auditors apply fines or judgments?*
Non-Compliance	How much risk will result due to non-compliance (ITP, Management Directives, Regulatory requirements)? 1. Minor / Moderate finding 2. Major finding 3. Fines against the agency 4. Loss of federal access/data/grants	*Is audit compliance a priority? Are your auditors aggressive or supportive? How will non-compliance affect the agency, project, or funding?*
Reputation Damage	Would a service disruption, data manipulation, data exposure, etc. result in reputation damage that would harm the business? 1. None 2. Minor damage 3. Moderate damage 4. Major damage	*Always linked to another loss. What will the response be from secondary stakeholders? E.g., auditors, the media, citizens, governor's office, legislature, etc.? For accuracy, can you quantify this in media/PR spend?*
Privacy Violation	How many closed records, e.g., personally identifiable information could be disclosed? 1. Less than 100 records 2. Hundreds of records 3. Thousands of records 4. Millions of records	*What is the number of records in the system currently? If a new system, how many do you foresee being entered into the system in the first year?*

Health, Safety, Welfare	Would a service disruption or data exposure result in negatively impacting the health, safety, or welfare of commonwealth citizens or employees? 1. Less than 100 records 2. Hundreds of records 3. Thousands of records 4. Millions of records	*What is the Service Level Agreement? Are there any redundant systems from other state or federal agencies?*
Operational Risk	Would a service disruption result in a degree of disruption of business operations? 1. Secondary operations interrupted 2. Minimal or temporary interruption to essential operations 3. Extensive interruption to secondary operations 4. Extensive essential operations interrupted 5. Essential and secondary operations interrupted	*What is the Service Level Agreement?* *Is this a mission critical application?* *Have you engaged OA/IT for a business impact analysis?*