pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Software Licensing Risk Assessment and Acknowledgment

Number
OPD-SFT001B

Effective Date
November 27, 2023

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
November 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.

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 Agency 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 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 **software requestor in consultation with Agency Legal Counsel and the Delivery Group or Agency Information Security Officer (ISO)** to document policy non-compliance and associated risk. Information shall be used by Agency Business Owners to make well informed decisions about risk.

Section 2: Risk Acknowledgement

Part VI - VII shall 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	
If cloud-based service, Cloud Use Case Title (SR#xxxxx)	
Asset(s):	
Most Restrictive Data (refer to ITP-SEC019)	
Affected Organization	

Risk Summary	Risk ID Refer to Table 1	Initial Risk	Risk Recommendation	Target Remediation	Remediation Contact

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	Compensating Controls	Residual Risk	Consequence	Corrective Action	Remediation Timeframe

Part III – Probability of Occurrence within in the first year
(Risk Exposure = Impact * Probability)

- High – Will probably occur in most circumstances within the next year
- Moderate – Might occur at some time within the next year
- Low – Could occur at some time

Risk Rating Enter High, Moderate, or Low	**Risk ID** Refer to Table 1	**Rationale** 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				

Section 2: Risk Acknowledgement

Part V - Risk to Business (Risk Exposure = Probability * Impact)		
Risk Category	**Risk Question**	**Response**
Contractual Risk	What is the potential impact to the Commonwealth resulting from a lack of a negotiated software agreement or accepting the Vendor's standard terms.	

Part VI – 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 Legal Counsel	<Insert Name - Required>	<MM/DD/YYYY>

Table 1 – Risk IDs

Table 1 Risk IDs – Legal Terms	
Legal Terms 1	IT Terms and Conditions
Legal Terms 2	Software License Agreement
Legal Terms 3	Non-Commonwealth Requirements for Applications/Services
Legal Terms 4	Vendor's EULA/Agreement

INSTRUCTIONS

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	
If cloud-based service, Cloud Use Case Title (SR#xxxxx)	
Asset(s):	*The thing we're trying to protect*
Most Restrictive Data	*Data categorization & Classification per ITP-SEC019*
Affected Organization	*Affected Organization Enter the line of business name or Enterprise if the entire Commonwealth is at risk.*

Risk Summary	Risk ID	Initial Risk	Risk Recommendation	Target Remediation	Remediation Contact
Specific risk scenario 1	*Risk ID from Table 1*	*From Risk Register or this Assessment – High, Moderate, or Low*	*Go, No-Go, or Proceed with Controls*	*Pre Go-Live, or Post Go-live*	*A person, not office or resource account*
Specific risk scenario 2	*Risk ID from Table 1*	*High, Moderate, or Low*	*Go, No-Go, or Proceed with Controls*	*Pre Go-Live, or Post Go-live*	*A person, not office or resource account*
	List each risk ID on a new line				

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	Compensating Controls	Residual Risk	Consequence	Corrective Action	Remediation Timeframe
Risk ID from Table 1	*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	*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 – Probability of Occurrence within in the first year

(Risk Exposure = Impact * Probability)

- High – Will probably occur in most circumstances within the next year
- Moderate – Might occur at some time within the next year
- Low – Could occur at some time

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

High, Moderate, or Low	*Risk ID from Table 1*	*Estimate probability, include assumptions, rationale, 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**
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*
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*

Risk Acknowledgement:

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

Part V - Risk to Business (Risk Exposure = Probability * Impact)		
Risk Category	**Risk Question**	**Response**
Contractual Risk	What is the potential impact to the Commonwealth resulting from a lack of a negotiated software agreement or accepting the Vendor's standard terms.	*Consider the potential impacts related to:* *Interruption of service* *What is the potential for litigation?* *Financial impacts - will there be recourse if issues arise?*