pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Risk Assessment and Acknowledgment

ITP Number OPD-SEC040A	**Effective Date** July 18, 2018
Category Security	**Supersedes** OPD-BUS011A
Contact RA-ITCentral@pa.gov	**Scheduled Review** January 2023

This point-in-time Risk Assessment and Acknowledgement document evidences that Agency Business Owners have been notified of, understand, and acknowledge the risk(s) associated with procuring and/or implementing this business and technology solution and/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 they are accepting the risk(s) as identified within this form and that in the event an issue occurs, they will accept responsibility for the risk(s) that were outlined and accepted 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 they are accepting the risk(s) as identified within this form and that in the event an issue occurs, they will accept responsibility for the risk(s) that were outlined and accepted 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 **Delivery Group and/or Agency CISO** 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 and/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				

Part V – CISO 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 CISO	<Insert Name – Required>	<MM/DD/YYYY>

Section 2: Risk Acknowledgement

Part VI - Risk to Business (Risk Exposure = Probability * Impact)		
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 Legal 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 Requirements
CSR-L2	Legal Review
CSR-L3	Access to Commonwealth specific systems, data, and services
CSR-L4	Data Hosting
CSR-L5	System and Organization Controls (SOC) Reporting. Include risk related to any exceptions or findings from SOC Reports.
CSR-S1	System Monitoring / Audit Logging (Security)
CSR-S2	Data Segmentation / Boundary Protection
CSR-S3	Exploit and Malware Protection
CSR-S4	Encryption
CSR-S5	Identity & Access Management
CSR-S6	Vulnerability Assessment
CSR-S7	Data Protection / 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 800-53 Control or NIST 800-171 Controls	List applicable NIST 800-53 Control Family(ies) (e.g., CA-1, RA-5).
Legal Terms (indicate 1, 2, 3, and/or 4)	1 - IT Terms and Conditions, 2- Software License Agreement, 3 - Non-Commonwealth Requirements for Applications/Services, 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*	*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*
	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, threat community motives, etc. Calibrate the estimate*

High, Moderate, or Low	*Risk ID from Table 1*	*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**
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 VI - Risk to Business (Risk Exposure = Probability * Impact)		
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	*Is audit compliance a priority? Are your auditors aggressive or supportive? How will non-compliance affect the agency, project, or funding?*

	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	*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 OIT for a business impact analysis?*