RISK ASSESSMENT REPORT TEMPLATE

Information Technology Risk Assessment For

Risk Assessment Annual Document Review History

The Risk Assessment is reviewed, at least annually, and the date and reviewer recorded on the table below.

Review Date	Reviewer

Table of Contents

List of Exhibits

List of Figures

List of Tables

1 INTRODUCTION

Risk assessment participants:

Participant roles in the risk assessment in relation assigned agency responsibilities:

Risk assessment techniques used:

Table A: Risk Classifications

Risk Level	Risk Description & Necessary Actions
High	**The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.**
Moderate	**The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.**
Low	**The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.**

2 IT SYSTEM CHARACTERIZATION

2 IT SYSTEM CHARACTERIZATION

Table B: IT System Inventory and Definition

IT System Inventory and Definition Document				
I. IT System Identification and Ownership				
IT System ID		**IT System Common Name**		
Owned By				
Physical Location				
Major Business Function				
System Owner Phone Number		**System Administrator(s) Phone Number**		
Data Owner(s) Phone Number(s)		**Data Custodian(s) Phone Number(s)**		
Other Relevant Information				
II. IT System Boundary and Components				
IT System Description and Components				
IT System Interfaces				
IT System Boundary				
III. IT System Interconnections (add additional lines, as needed)				
Agency or Organization	**IT System Name**	**IT System ID**	**IT System Owner**	**Interconnection Security Agreement Status**

Table B: IT System Inventory and Definition (continued)

Overall IT System Sensitivity Rating and Classification	**Overall IT System Sensitivity Rating** Must be "high" if sensitivity of any data type is rated "high" on any criterion		
	HIGH	**MODERATE**	**LOW**
	IT System Classification Must be "Sensitive" if overall sensitivity is "high"; consider as "Sensitive" if overall sensitivity is "moderate"		
	SENSITIVE		**NON-SENSITIVE**

Description or diagram of the system and network architecture, including all components of the system and communications links connecting the components of the system, associated data communications and networks:

Figure 1 – IT System Boundary Diagram

Description or a diagram depicting the flow of information to and from the IT system, including inputs and outputs to the IT system and any other interfaces that exist to the system:

Figure 2 – Information Flow Diagram

3 RISK IDENTIFICATION

Identification of Vulnerabilities

Vulnerabilities were identified by:

Identification of Threats

Threats were identified by:

The threats identified are listed in Table C.

Table C: Threats Identified

Identification of Risks

Risks were identified by:

The way vulnerabilities combine with credible threats to create risks is identified Table D.

Table D: Vulnerabilities, Threats, and Risks

Risk No.	Vulnerability	Threat	Risk of Compromise of	Risk Summary
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

4 CONTROL ANALYSIS

Table E documents the IT security controls in place and planned for the IT system.

Table E: Security Controls

Control Area	In-Place/ Planned	Description of Controls
1 Risk Management		
1.1 IT Security Roles & Responsibilities		
1.2 Business Impact Analysis		
1.3 IT System & Data Sensitivity Classification		
1.4 IT System Inventory & Definition		
1.5 Risk Assessment		
1.6 IT Security Audits		
2 IT Contingency Planning		
2.1 Continuity of Operations Planning		
2.2 IT Disaster Recovery Planning		
2.3 IT System & Data Backup & Restoration		
3 IT Systems Security		
3.1 IT System Hardening		
3.2 IT Systems Interoperability Security		
3.3 Malicious Code Protection		
3.4 IT Systems Development Life Cycle Security		
4 Logical Access Control		
4.1 Account Management		

Control Area	In-Place/ Planned	Description of Controls
4.2 Password Management		
4.3 Remote Access		
5 Data Protection		
4.4 Data Storage Media Protection		
4.5 Encryption		
6 Facilities Security		
6.1 Facilities Security		
7 Personnel Security		
7.1 Access Determination & Control		
7.2 IT Security Awareness & Training		
7.3 Acceptable Use		
8 Threat Management		
8.1 Threat Detection		
8.2 Incident Handling		
8.3 Security Monitoring & Logging		
9 IT Asset Management		
9.1 IT Asset Control		
9.2 Software License Management		
9.3 Configuration Management & Change Control		

Table E correlates the risks identified in Table C with relevant IT security controls documented in Table D and with other mitigating or exacerbating factors.

Table F: Risks-Controls-Factors Correlation

Risk No.	Risk Summary	Correlation of Relevant Controls & Other Factors
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		

5 RISK LIKELIHOOD DETERMINATION

Table G defines the risk likelihood ratings.

Table G: Risk Likelihood Definitions

Effectiveness of Controls	Probability of Threat Occurrence (Natural or Environmental Threats) or Threat Motivation and Capability (Human Threats)		
	Low	Moderate	High
Low	Moderate	High	High
Moderate	Low	Moderate	High
High	Low	Low	Moderate

Table G, evaluates the effectiveness of controls and the probability or motivation and capability of each threat to BFS and assigns a likelihood, as defined in Table F, to each risk documented in Table C.

Table H: Risk Likelihood Ratings

Risk No.	Risk Summary	Risk Likelihood Evaluation	Risk Likelihood Rating
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

Risk No.	Risk Summary	Risk Likelihood Evaluation	Risk Likelihood Rating
20			
21			
22			
23			
24			
25			

6 IMPACT ANALYSIS

Table I documents the ratings used to evaluate the impact of risks.

Table I: Risk Impact Rating Definitions

Magnitude of Impact	Impact Definition
High	Occurrence of the risk: (1) may result in human death or serious injury; (2) may result in the loss of major COV tangible assets, resources or sensitive data; or (3) may significantly harm, or impede the COV's mission, reputation or interest.
Moderate	Occurrence of the risk: (1) may result in human injury; (2) may result in the costly loss of COV tangible assets or resources; or (3) may violate, harm, or impede the COV's mission, reputation or interest.
Low	Occurrence of the risk: (1) may result in the loss of some tangible COV assets or resources or (2) may noticeably affect the COV's mission, reputation or interest.

Table J documents the results of the impact analysis, including the estimated impact for each risk identified in Table D and the impact rating assigned to the risk.

Table J: Risk Impact Analysis

Risk No.	Risk Summary	Risk Impact	Risk Impact Rating
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

Risk No.	Risk Summary	Risk Impact	Risk Impact Rating
18			
19			
20			
21			
22			
23			
24			
25			

Description of process used in determining impact ratings:

7 RISK DETERMINATION

Table K documents the criteria used in determining overall risk ratings.

Table K: Overall Risk Rating Matrix

Risk Likelihood	Risk Impact		
	Low (10)	Moderate (50)	High (100)
High (1.0)	Low 10 x 1.0 = 10	Moderate 50 x 1.0 = 50	High 100 x 1.0 = 100
Moderate (0.5)	Low 10 x 0.5 = 5	Moderate 50 x 0.5 = 25	Moderate 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Risk Scale: Low (1 to 10); Moderate (>10 to 50); High (>50 to 100)

Table L assigns an overall risk rating, as defined in Table K, to each of the risks documented in Table D.

Table L: Overall Risk Ratings Table

Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
21				
22				
23				
24				
25				

Description of process used in determining overall risk ratings:

8 RECOMMENDATIONS

Table M documents recommendations for the risks identified in Table D.

Table M: Recommendations

Risk No.	Risk	Risk Rating	Recommendations
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

9 RESULTS DOCUMENTATION

Exhibit 1: Risk Assessment Matrix

Risk No.	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls and Other Factors	Recommendations
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									