

## **COMMONWEALTH OF VIRGINIA**



# **Information Technology Resource Management Information Technology Risk Management Guideline**

## **Appendix D – Risk Assessment Instructions**

Virginia Information Technologies Agency (VITA)

**TABLE OF CONTENTS**

**PURPOSE, CAUTIONS & FORMAT .....1**  
**EXAMPLE RISK ASSESSMENT .....2**  
**RISK ASSESSMENT REPORT TEMPLATE .....37**

# PURPOSE, CAUTIONS & FORMAT

## PURPOSE

This document contains instructions to implement the methodology described in Section 6 (Risk Assessment) of the Information Technology (IT) Risk Management Guideline, ITRM Guideline SEC5506-01. This document is Appendix D of that Guideline, and is published under separate cover because of its size. This template does not stand alone and should be read only in conjunction with the Guideline.

The purpose of this document is to assist each Commonwealth of Virginia (COV) Agency in assessing the risks to its sensitive IT systems and data, and protecting the resources that support the Agency's mission. These instructions are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, "Risk Management Guide for Information Technology Systems" and contain a recommended format for COV risk assessments.

## CAUTIONS REGARDING USE OF THIS DOCUMENT

The example risk assessment in this document:

1. Does not document compliance with all requirements of the COV ITRM *IT Security Policy, IT Security Standard and IT Security Audit Standard*. These omissions are designed to illustrate control weaknesses, and must not be construed to relieve any COV Agency of its responsibility to comply with all applicable requirements of *IT Security Policy, IT Security Standard and IT Security Audit Standard*.
2. Contains the names of fictional individuals, corporations, and products. No similarity to any actual persons, living or dead, nor to any actual corporation or product, past, present, or future, is intended. In addition no such similarity to any actual corporation or product, past, present, or future may be construed to represent an endorsement of any such corporation or product.

## FORMAT

This document uses different fonts for instructions and examples, as follows:

- Times New Roman text, including all of the text in this section, is provided as instructions for completing a risk assessment.
- **Arial Bold text** inside a shaded text border is example text. In the examples, the template uses a fictional system called the Budget Formulation System (BFS), owned and operated by the Financial Operations Division (FOD) of a fictional agency called the Budget Formulation Agency (BFA).
- *Times New Roman italic text* is provided as background information. It is provided for better understanding of how to complete each section of the Risk Assessment Report, or so that the

author knows to extend or replicate a section, such as by adding Agency-specific threats or vulnerabilities to the risk matrix.

This document consists of two primary sections:

- An example risk assessment, with instructions and explanatory material for BFS. This section is intended to provide guidance to COV agencies on how to complete risk assessments of their sensitive IT systems.
- A blank Risk Assessment Report containing the section headings and tables from the recommended format Risk Assessment Report, but no content. This section is intended for use by COV agencies in completing Risk Assessment Reports for their sensitive systems.

## **EXAMPLE RISK ASSESSMENT**

The example Risk Assessment begins with the cover sheet on the following page.

**Example Risk Assessment Report  
Information Technology Risk  
Assessment For**

**Budget Formulation Agency  
Budget Formulation System**

**Version 1.0**

**July 2007**

**Prepared For:**

**Budget Formulation Agency  
Financial Operations Division  
123 E. Elm Street  
Richmond, VA 23299**

**Prepared By:**

**Budget Formulation Agency  
Financial Operations Division  
123 E. Elm Street  
Richmond, VA 23299**

# Example Risk Assessment Report

## *Risk Assessment Annual Document Review History*

<b>Review Date</b>	<b>Reviewer</b>
<b>July, 2005</b>	<b>Jane Jones</b>
<b>July, 2006</b>	<b>Jane Jones</b>

The conditions of the risk assessment change as the agency's business environment changes. Review the risk assessment annually (or more frequently) to reflect those changes and improve the validity of the assessment.

# Example Risk Assessment Report

## TABLE OF CONTENTS

1	INTRODUCTION .....	7
2	IT SYSTEM CHARACTERIZATION .....	9
3	RISK IDENTIFICATION .....	14
4	CONTROL ANALYSIS .....	20
5	RISK LIKELIHOOD DETERMINATION .....	32
6	RISK IMPACT ANALYSIS.....	35
7	OVERALL RISK DETERMINATION.....	38
8	RECOMMENDATIONS.....	41
9	RESULTS DOCUMENTATION.....	44

## LIST OF EXHIBITS

EXHIBIT 1: RISK ASSESSMENT MATRIX .....	45
---	----

## LIST OF FIGURES

FIGURE 1: IT SYSTEM BOUNDARY DIAGRAM.....	13
FIGURE 2: INFORMATION FLOW DIAGRAM .....	13

# Example Risk Assessment Report

## LIST OF TABLES

<b>TABLE A: RISK CLASSIFICATIONS.....</b>	<b>8</b>
<b>TABLE B: ITSYSTEM INVENTORY AND DEFINITION .....</b>	<b>9</b>
<b>TABLE C: THREATS IDENTIFIED .....</b>	<b>16</b>
<b>TABLE D: THREATS, VULNERABILITIES, AND RISKS .....</b>	<b>18</b>
<b>TABLE E: SECURITY CONTROLS.....</b>	<b>21</b>
<b>TABLE F: RISKS-CONTROLS-FACTORS CORRELATION.....</b>	<b>30</b>
<b>TABLE G: RISK LIKELIHOOD DEFINITIONS.....</b>	<b>32</b>
<b>TABLE H: RISK LIKELIHOOD RATINGS.....</b>	<b>33</b>
<b>TABLE I: RISK IMPACT RATING DEFINITIONS .....</b>	<b>35</b>
<b>TABLE J: RISK IMPACT ANALYSIS .....</b>	<b>36</b>
<b>TABLE K: OVERALL RISK RATING MATRIX .....</b>	<b>39</b>
<b>TABLE L: OVERALL RISK RATINGS TABLE.....</b>	<b>39</b>
<b>TABLE M: RECOMMENDATIONS.....</b>	<b>42</b>

# Example Risk Assessment Report

## 1 INTRODUCTION

The introduction should briefly describe the purpose of this risk assessment and include a brief description of the approach used to conduct the risk assessment. The description of the approach should include:

- The participants and their roles in the risk assessment in relation to their assigned responsibilities at the agency;
- The techniques used to gather the necessary information (e.g., the use of tools, questionnaires); and
- The risk classifications used.

Agencies are encouraged to classify risks as High, Moderate or Low in accordance with the definitions in the Standard<sup>1</sup>. The definitions of risk classifications should be included in Table A of the Risk Assessment Report.

### 1 Introduction

**Staff of the Commonwealth of Virginia (COV) Budget Formulation Agency (BFA) performed this risk assessment for the Budget Formulation System (BFS) to satisfy the requirement of ITRM Standard SEC501-01 to perform an assessment at least every 3 years or whenever a major change is made to a sensitive system. The last risk assessment for this system was completed on July 10, 2004.**

**This risk assessment builds upon earlier risk assessments performed by the Budget Formulation Agency staff. In addition, an IT Security Audit, conducted by BFA Internal Audit Services staff on June 24, 2007 was utilized. This risk assessment was performed in accordance with a methodology described in ITRM Guideline SEC50X-0X, and utilized interviews and questionnaires developed by BFA staff to identify BFS**

- **Vulnerabilities;**
- **Threats;**
- **Risks;**
- **Risk Likelihoods; and**
- **Risk Impacts.**

**In addition, the risk assessment utilized ITRSK, an automated risk assessment tool.**

**Participants and their roles in this risk assessment included the following:**

- **Jane Jones, BFA Information Security Officer, reviewed the Risk Assessment report prior to completion;**

---

<sup>1</sup> These definitions are based on definition in Federal Information Processing Standards Publication 199 (FIPS 199)

# Example Risk Assessment Report

- **John James, BFS System Owner, managed the risk assessment process, using BFA Information Risk Management staff to conduct the risk assessment, as well as providing information through interviews and completing questionnaires.**
- **Mike Williams, BFS Data Owner, provided information through interviews and through completing questionnaires;**
- **Bill Michaels, BFS Data Owner, provided information through interviews and through completing questionnaires;**
- **Bea Roberts, of Partner Systems, Inc. (PSI), BFS Data Custodian, operational and technical support staff, and BFS System Administrators provided required technical information regarding BFS, and provided information through interviews and questionnaires.**

*Table A defines the risk levels (high, moderate, low) adopted to classify risks to the Agency, in the context of the BIA.*

<b>Table A: Risk Classifications</b>	
<b>Risk Level</b>	<b>Risk Description</b>
<b>High</b>	<b>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.</b>
<b>Moderate</b>	<b>The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.</b>
<b>Low</b>	<b>The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.</b>

# Example Risk Assessment Report

## 2 IT SYSTEM CHARACTERIZATION

IT system characterization defines the scope of the risk assessment effort. Use the previously-developed IT System Inventory and Definition Document (Appendix B of the Guideline) as input for this step; some additional information is required. The purpose of this step is to identify the IT system, to define the risk assessment boundary and components, and to identify the IT system and data sensitivity

### 2 BFS Identification

#### 2.1 IT System Identification

Include in the Risk Assessment Report the previously developed IT System Inventory and Definition Document.

**Table B: IT System Inventory and Definition**

IT System Inventory and Definition Document			
I. IT System Identification and Ownership			
IT System ID	BFA-001	IT System Common Name	Budget Formulation System (BFS)
Owned By	Budget Formulation Agency (BFA) Financial Operations Division (FOD)		
Physical Location	BFA Data Center 123 E. Elm Street, Richmond, VA 23299		
Major Business Function	Enable processing of current-year budget details and future-year budget plans		
System Owner Phone Number	John James (804) 979-3757	System Administrator(s) Phone Number	Partner Systems, Inc. (888) 989-8989
Data Owner(s) Phone Number(s)	Mike Williams (804) 979-3452 Bill Michaels (804) 979-3455	Data Custodian(s) Phone Number(s)	Bea Roberts Partner Systems, Inc. (888) 989-8989
Other Relevant Information	BFS has been in production since December 1996		

# Example Risk Assessment Report

**Table B: System Inventory and Definition (continued)**

II. IT System Boundary and Components	
IT System Description and Components	<p>BFS is a distributed client-server application transported by a network provided by PSI, a third-party. The major components of the BFS include:</p> <ul style="list-style-type: none"> <li>• A Sparc SUNW, Ultra Enterprise 3500 server running SunOS 5.7 (Solaris 7). The server has four (4) processors running at 248 MHz, 2048 MB of memory, 4 SBus cards, 4 PCI cards, and total disk storage capacity of 368.6 GB (36 drives x 10 GB). This system is provided to BFA under contract by PSI, and this Risk Assessment relies on information regarding system hardware and Operating System software provided to BFA by PSI.</li> <li>• One (1) network interface that is connected to BFA's data center Cisco switch. This interface is assigned two unique IP addresses.</li> <li>• An Oracle 9i data store with two (2) commercial off-the-shelf (COTS) application modules (ABC and XYZ) purchased from Oracle Corporation.</li> </ul>
IT System Interfaces	<ul style="list-style-type: none"> <li>• An interface between BFS and the Budget Consolidation System (BCS). This interface allows only the BCS to securely transmit data using the Secure Copy Protocol (SCP) on port 22 into the BFS nightly by a cron job that refreshes tables in the BFS Oracle store with selected data from BCS tables.</li> <li>• A modem for emergency dial-in support and diagnostics, secured via the use of a one-time password authentication mechanism.</li> <li>• Client software located within the Agency's Windows 2003 Server Active Directory Domain to manage access to BFS. This software utilizes encrypted communications between the client and the server and connects to the server on port 1521. Only users with the appropriate rights within the BFA Domain can access the client software, although a separate client login and password is required to gain access to BFS data and functions. This access is based on Oracle roles and is granted by the BFS system administrators to users based on their job functions.</li> </ul>
IT System Boundary	<ul style="list-style-type: none"> <li>• The demarcation between the BFS and the Local Area Network (LAN) is the physical port on the Cisco switch that connects the BFS to the network. The switch and other network components are not considered to be part of the BFS.</li> <li>• BFS support personnel provide the operation and maintenance of the application. The BFS personnel provide the operation and maintenance of the server and operating system. The BFS boundary is the following directories and their sub-directories: /var/opt/Oracle, /databases/Oracle, and /opt/odbc. Other directories are outside the BFS boundary.</li> <li>• BFS is responsible for receiving data from the BCS. The BCS is a separate system and is outside the BFS boundary.</li> <li>• Client access to the BFS server is controlled by BFA's Windows 2003 Server Active Directory domain. This access are included within the BFS system boundary. The overall BFA Windows 2003 Server Active Directory domain, however, is not considered to be part of the BFS, and is outside the BFS boundary.</li> </ul>

# Example Risk Assessment Report

**Table B: System Inventory and Definition (continued)**

III. IT System Interconnections				
Agency or Organization	IT System Name	IT System ID	IT System Owner	Interconnection Security Agreement Summary
BFA	Budget Consolidation System	BCS	John James	No formal agreement required, as systems have common owner
Partner Services, Inc. (PSI)	Enterprise Data Network	EDN	Bea Roberts	Agreement is in place; expires 12/31/2007; under renegotiation
IV. IT System and Data Sensitivity				
Type of Data	Sensitivity Ratings Include Rationale for each Rating			
	Confidentiality	Integrity	Availability	
Current Year Budget Details	Low Data is public information	High BFS is system of record for fiscal year budget data for all COV Agencies	Moderate Data is used less than daily by all COV Agencies to allocate resources	
Future Year Budget Plans	High Release of the data before it is final could be damaging to COV and its Agencies	Moderate BFS is system of record for future year budget plans for all COV Agencies	Low/High Low during most of year; high during budget preparation	
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	

# Example Risk Assessment Report

## 2.2 IT System Boundary & Components included in the Risk Assessment

Using the system boundary information already documented in Table B (see Section 3.2.3 of the Guideline), verify that the components that are included in this risk assessment are defined, and components not included are defined as appropriate. If the IT System under assessment connects or shares data with other IT Systems, risks associated with these other IT Systems should be considered in the risk assessment, even though the other IT Systems themselves will not be reassessed.

*In most cases, the components included in the risk assessment will be the same as those within the system boundary (see section 3.2.3 of the Risk Management Guideline). Agencies, however, must make an affirmative decision regarding components included in the risk assessment, including major components that could create risk for the IT system.*

*For example, an IT system (System A) may make use of a third-party network infrastructure, but since the third-party network is subject to a separate risk assessment, should not be assessed again. However, the System A risks assessment should reference the network risk assessment, and highlight any pertinent network risks. Establishing parameters in which the system operates guarantees consideration of all relevant threats, vulnerabilities and risks, and an explicit decision as to the scope of the assessment.*

*The key part of defining the components included in the risk assessment is to look at where IT systems meet and to define where the dividing line is located. This applies not only to physical connections, but also to logical connections where data is exchanged. The owner(s) of this system and the owner(s) of the interconnected systems must agree on the components included in the risk assessment of each system, so that all components are the responsibility of someone, and no components are covered more than once. In the event that the IT system serves more than one Agency, the details of this use should be clearly defined in a written agreement. The agreement between system owners should be based on non-arbitrary characteristics, such as funding boundaries, functional boundaries, physical gaps, contractual boundaries, operational boundaries and transfer of information custody.*

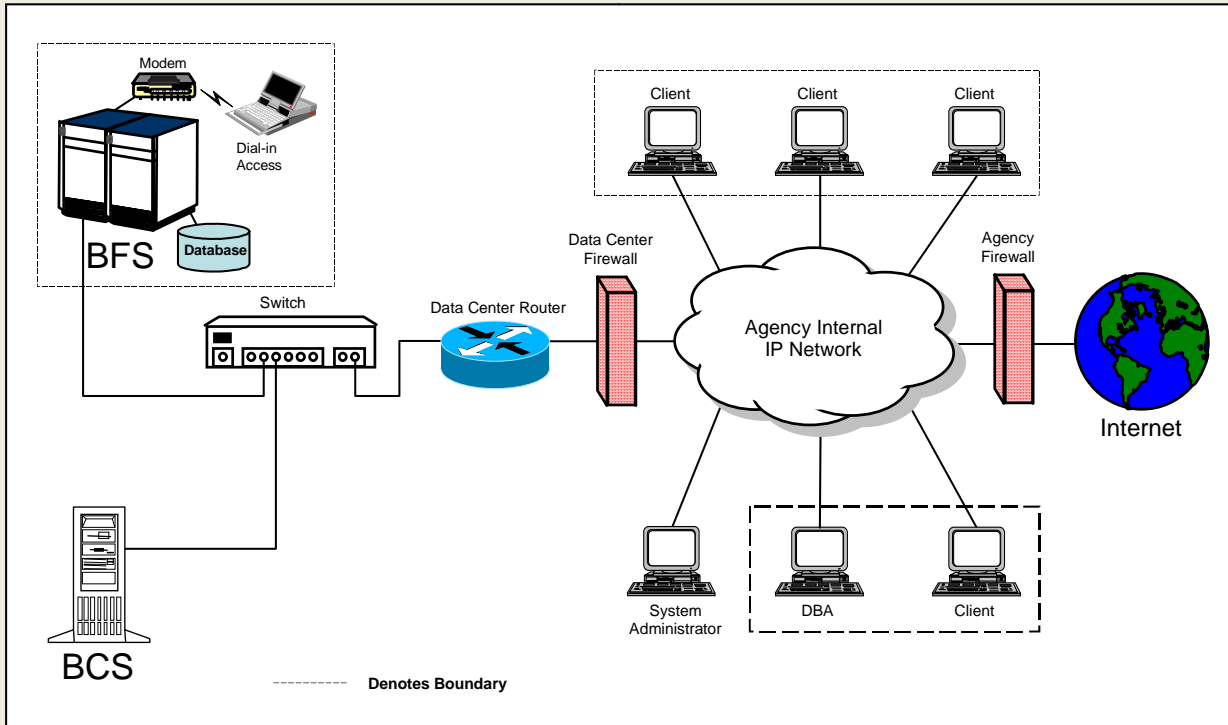
## 2.3 Additional IT System Documentation

In addition to the System Inventory and Definition document, include in this section of the Risk Assessment Report:

- A 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.
- A 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.

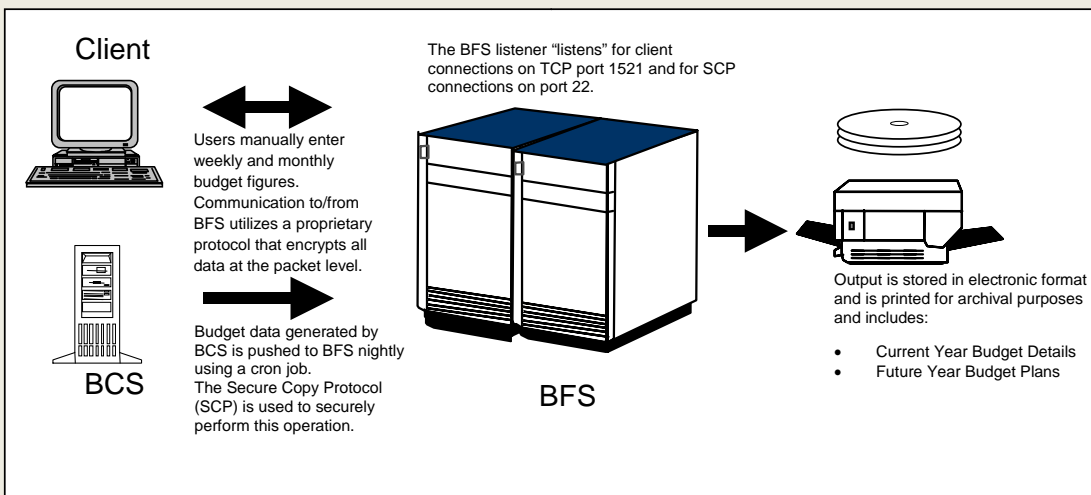
# Example Risk Assessment Report

Figure 1: IT System Boundary Diagram



A high-level diagram depicting the BFS information flow is provided in Figure 2.

Figure 2: Information Flow Diagram



# Example Risk Assessment Report

## 3 RISK IDENTIFICATION

The purpose of this step is to identify the risks to the IT system. Risks occur in IT systems when vulnerabilities (i.e., flaws or weaknesses) in the IT system or its environment can be exploited by threats (i.e. natural, human, or environmental factors).

*For example, Oracle 9i will stop responding when sent a counterfeit packet larger than 50,000 bytes. This flaw constitutes a vulnerability. A malicious user or computer criminal might exploit this vulnerability to stop an IT system from functioning. This possibility constitutes a threat. This vulnerability-threat pair combines to create a risk that an IT system could become unavailable.*

The process of risk identification consists of three components:

1. Identification of vulnerabilities in the IT system and its environment;
2. Identification of credible threats that could affect the IT system; and
3. Pairing of vulnerabilities with credible threats to identify risks to which the IT system is exposed.

*After the process of risk identification is complete, likelihood and impact of risks will be considered.*

### 3 Risk Identification

#### 3.1 Identification of Vulnerabilities

The first component of risk identification is to identify vulnerabilities in the IT system and its environment. There are many methodologies or frameworks for determining IT system vulnerabilities. The methodology should be selected based on the phase of the IT system is in its life cycle. For an IT system:

- In the Project Initiation Phase, the search for vulnerabilities should focus on the organizations IT security policies, planned procedures and IT system requirements definition, and the vendor's security product analyses (e.g., white papers).
- In the Project Definition Phase, the identification of vulnerabilities should be expanded to include more specific information. Assess the effectiveness of the planned IT security features described in the security and system design documentation.
- In the Implementation Phase, the identification of vulnerabilities should also include an analysis of the security features and the technical and procedural security controls used to protect the system. These evaluations include activities such as executing a security self-assessment, the effective application of automated vulnerability scanning/assessment tools and/or conducting a third-party penetration test. Often, a mixture of these and other methods is used to get a more comprehensive list of vulnerabilities.

# Example Risk Assessment Report

Include in the Risk Assessment Report a description of how vulnerabilities were determined. If a Risk Assessment has been performed previously, it should contain a list of vulnerabilities that should be assessed to determine their continued validity. In addition, assess and document if any new vulnerabilities exist.

## 3.1 Identification of Vulnerabilities

**BFS is in the implementation phase of its life cycle. Accordingly, identification of vulnerabilities for BFS included:**

- Interviews with the BFA System Owner, Data Owner, and BFA operational and technical support personnel;
- Use of the automated ITRSK tool; and
- Review of vulnerabilities identified in the previous BFA Risk Assessment.

Vulnerabilities that combine with credible threats (see Section 3.2) create a risk to the IT system that will be listed in step 3.3

## 3.2 Identification of Credible Threats

The purpose of this component of risk identification is to identify the credible threats to the IT system and its environment. A threat is credible if it has the potential to exploit an identified vulnerability.

Table C, at the end of this section, contains examples of threats. The threats listed in the table are provided only as an example and are specific to the example BFS system. Agencies are encouraged to consult other threat information sources, such as NIST SP 800-30. The goal is to identify all credible threats to the IT system, but not to create a universal list of general threats.

Include in the Risk Assessment Report a description of how threats were determined. If a Risk Assessment has been performed previously, it should contain a list of credible threats that must be assessed to determine their continued validity. In addition, assess and document if any new vulnerabilities exist.

Include a brief description of how credible threats were determined and a list of the credible threats in the Risk Assessment Report.

# Example Risk Assessment Report

## 3.2 Identification of Credible Threats

Credible threats to the Budget Formulation System were identified by:

- Consulting the previous BFS Risk Assessment and analyzing how the BFS threat environment has changed in the past three years;
- Interviewing the BFS System Owner, Data Owner, and System Administrators to gather information about system-specific threats to the BFS; and
- Use of the automated ITRSK tool to identify threats to the BFS.

**Table C: Credible Threats Identified for the BFS**

Air Conditioning Failure	Earthquakes	Nuclear Accidents
Aircraft Accident	Electromagnetic Interference	Pandemic
Biological Contamination	Fire (Major or Minor)	Power Loss
Blackmail	Flooding/Water Damage	Sabotage
Bomb Threats	Fraud/Embezzlement	Terrorism
Chemical Spills	Hardware Failure	Tornados, Hurricanes, Blizzards
Communication Failure	Human Error	Unauthorized Access or Use
Computer Crime	Loss of Key Personnel	Vandalism and/or Rioting
Cyber-Terrorism	Malicious Use	Workplace Violence

## 3.3 Identification of Risks

The final component of risk identification is to pair identified vulnerabilities with credible threats that could exploit them and expose the following to significant risk:

- IT system;
- The data it handles; and
- The organization.

*In order to focus risk management efforts on those risks that are likely to materialize, it is important both to be comprehensive in developing the list of risks to the IT system and also to limit the list to pairs of actual vulnerabilities and credible threats. For example, as noted at the beginning of section 3, Oracle 9i will stop responding when sent a counterfeit packet larger than 50,000 bytes. This flaw constitutes vulnerability. A malicious user or computer criminal might exploit this vulnerability to stop an IT system from functioning. This possibility constitutes a*

# Example Risk Assessment Report

*threat. This vulnerability-threat pair combines to create a risk that an IT system could become unavailable.*

*If an IT system running Oracle 9i is not connected to a network, however, such as the certificate authority for a Public Key Infrastructure (PKI) system, then there is no credible threat, and so no vulnerability-threat pair to create a risk.*

Provide a brief description of how the risks were identified, and prepare a table of all risks specific to this IT system. In the table, each vulnerability should be paired with at least one appropriate threat, and a corresponding risk. The risks should be numbered and each risk should include a description of the results if the vulnerability was to be exploited by the threat. Enter the data into Exhibit 1 (this data entry can be done by means of cutting and pasting).

### **3.3 Identification of Risks**

**Risks were identified for the BFS by matching identified vulnerabilities with credible threats that might exploit them. This pairing of vulnerabilities with credible threats is documented in Table D. All identified risks have been included.**

Table D, on the next page, documents example vulnerabilities, threats and risks for the BFS. The list in Table D is an example and pertains only to the fictional BFS.

# Example Risk Assessment Report

**Table D: Vulnerabilities, Threats, and Risks**

<b>Risk No.</b>	<b>Vulnerability</b>	<b>Threat</b>	<b>Risk of Compromise of</b>	<b>Risk Summary</b>
1	Wet-pipe sprinkler system in BFS Data Center.	Fire	Availability of BFS and data.	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.
2	BFS user identifiers (IDs) no longer required are not removed from BFS in timely manner.	Unauthorized Use	Confidentiality & integrity of BFS data.	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.
3	BFS access privileges are granted on an ad-hoc basis rather than using predefined roles.	Unauthorized Access	Confidentiality & integrity of BFS data.	Unauthorized access via ad-hoc privileges could compromise confidentiality & integrity of BFS data.
4	Bogus TCP packets (> 50000 bytes) directed at port 1521 will cause BFS to stop responding.	Malicious Use Computer Crime	Availability of BFS and data.	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.
5	New patches to correct flaws in application security design have not been applied.	Malicious Use Computer Crime	Confidentiality & integrity of BFS data.	Exploitation of unpatched application security flaws could compromise confidentiality & integrity of BFS data.
6	User names & passwords are in scripts & initialization files.	Malicious Use Computer Crime	Confidentiality & integrity of BFS data.	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.
7	Passwords are not set to expire; regular password changes are not enforced.	Malicious Use Computer Crime	Confidentiality & integrity of BFS data.	Compromise of unexpired/unchanged passwords could result in compromise of confidentiality & integrity of BFS data.

# Example Risk Assessment Report

**Table D: Vulnerabilities, Threats, and Risks (continued)**

<b>Risk No.</b>	<b>Vulnerability</b>	<b>Threat</b>	<b>Risk of Compromise of</b>	<b>Risk Summary</b>
8	“Generic” accounts found in the database (e.g., test, share, guest).	Malicious Use Computer Crime	Confidentiality & integrity of BFS data.	Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data.
9	Remote OS authentication is enabled but not used.	Malicious Use Computer Crime	Confidentiality & integrity of BFS data.	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.
10	Login encryption setting is not properly configured.	Malicious Use Computer Crime	Confidentiality & integrity of BFS data.	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.
11	Sensitive BFS data is stored on USB drives	Malicious Use Computer Crime	Confidentiality of BFS data.	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.

# Example Risk Assessment Report

## 4 CONTROL ANALYSIS

The purpose of this step is to document a list of security controls used for the IT system. These controls should correspond to the requirements of the *Policy, Standard, and Audit Standard*. The analysis should also specify whether the control is in-place (i.e., current) or planned, and whether the control is currently enforced. In the next step these controls are matched with the risks identified in Table D, in order to identify those risks that require additional response.

*Table E is an example of a security controls list that corresponds to the requirements of the Policy, Standard, and Audit Standard. This list shows controls that are in-place, as well as those planned for implementation.*

### 4 Control Analysis

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

# Example Risk Assessment Report

**Table E: Security Controls**

Control Area	In-Place/ Planned	Description of Controls
<b>1 Risk Management</b>		
1.1 IT Security Roles & Responsibilities	In place	<ol style="list-style-type: none"> <li>1. Required IT Security roles have been assigned in writing, both for BFA as a whole, &amp; for the BFS. John Howard, BFA Commissioner, has designated Jane Jones as BFA ISO &amp; delegated the assignment of other IT security roles to her.</li> <li>2. With respect to BFS, Jane Jones has assigned individuals to the required IT security roles, as documented elsewhere in this report.</li> </ol>
1.2 Business Impact Analysis	In place	<ol style="list-style-type: none"> <li>1. BFA management &amp; staff conducted &amp; documented a Business Impact Analysis (BIA) of the Agency during June 2004; this BIA was updated in May 2007. The BFA BIA notes that the BFS supports essential BFA functions.</li> </ol>
1.3 IT System & Data Sensitivity Classification	In place	<ol style="list-style-type: none"> <li>1. BFA has documented classification of the sensitivity of BFA IT systems &amp; data, including the BFS. This classification notes the high sensitivity of much of the data handled by the BFS.</li> </ol>
1.4 IT System Inventory & Definition	In place	<ol style="list-style-type: none"> <li>1. BFA has documented an inventory of its sensitive IT systems; this inventory includes the BFS; the System Definition of BFS is included in Section 2 of this Risk Assessment report.</li> </ol>
1.5 Risk Assessment	In place  Planned	<ol style="list-style-type: none"> <li>1. This report documents the Risk Assessment of BFS in July 2007, building on an earlier BFS Risk Assessment in July 2004.</li> <li>2. BFA will validate the current Risk Assessment through annual self-assessments in July 2008 &amp; July 2009, &amp; will conduct the next formal BFS RA in July 2010, or sooner, if necessary.</li> </ol>
1.6 IT Security Audits	In place  Planned	<ol style="list-style-type: none"> <li>1. Anne Keller, BFA Internal Audit Director manages IT Security Audits for BFA.</li> <li>2. An IT Security Audit of BFS was conducted &amp; documented by BFA Internal Audit staff on June 24, 2007.</li> <li>3. Required reporting for the BFS CAP is in place.</li> <li>4. Future IT Security Audits of BFA are planned biennially.</li> </ol>
<b>2 IT Contingency Planning</b>		
2.1 Continuity of Operations Planning	In place  Planned	<ol style="list-style-type: none"> <li>1. Sam Robinson is the BFA Continuity of Operations Plan (COOP) Coordinator &amp; also serves as the focal point for IT COOP &amp; Disaster Recovery (DR) activities.</li> <li>2. The BFA COOP documents the requirements for 24-hour recovery of the BFS &amp; its data to support budget preparation, &amp; 72-hour recovery of BFS &amp; its data at other times.</li> <li>3. The BFA COOP identifies all personnel required for its execution, including personnel required for recovery of the BFS, &amp; includes emergency declaration, notification, &amp; operations procedures.</li> <li>4. The COOP document is classified as sensitive; access to this document is restricted to COOP team members, &amp; a copy of the COOP is stored off site at Data Recovery Services, Inc., BFA's recovery site partner.</li> <li>5. Recovery procedures for BFS were most recently tested during BFA's annual COOP exercise on May 18-20, 2007.</li> <li>6. The BFA COOP, including components relating to the BFS is currently being updated as a result of the COOP exercise; completion is expected by September 1, 2007.</li> <li>7. Recovery procedures for BFS will next be tested during the BFA COOP exercise scheduled for May 2008.</li> </ol>

# Example Risk Assessment Report

**Table E: Security Controls (continued)**

Control Area	In-Place/ Planned	Description of Controls
<b>2 IT Contingency Planning (continued)</b>		
2.2 IT Disaster Recovery Planning	In place	<ol style="list-style-type: none"> <li>1. A Disaster Recovery Plan (DRP) for the BFS has been documented &amp; approved by the BFA Commissioner. This plan calls for recovery of the BFS within 72 hours at a cold site maintained by with Data Recovery Services, Inc. (DRSI) through a contract with DRSI. In order to support 24-hour recovery of BFS during budget preparation, the contract with DRSI includes 24-hour recovery during this period.</li> <li>2. Both 72- &amp; 24-hour recovery of the BFS were tested during the BFA COOP exercise on May 18-20, 2007, including access to the recovered BFS by users at other COV Agencies. Members of the BFS Disaster Recovery Team received training on their responsibilities in advance of the exercise.</li> </ol>
	Planned	<ol style="list-style-type: none"> <li>1. The BFS DRP is currently being updated as a result of the recovery during the BFA COOP exercise; completion is expected by September 1, 2007.</li> <li>2. Recovery of the BFS will next be tested during the BFA COOP exercise scheduled for May 2008.</li> </ol>
2.3 IT System & Data Backup & Restoration	In place	<ol style="list-style-type: none"> <li>1. A Backup &amp; Restoration Plan for the BFS has been documented, &amp; approved by John James, the BFS System Owner. This plan calls for:               <ol style="list-style-type: none"> <li>a. Weekly full &amp; daily incremental backups &amp; review of backup logs of BFS data by operations staff;</li> <li>b. Weekly pickup &amp; transport of BFS backup tapes to DRSI by DRSI personnel; &amp;</li> <li>c. Restoration of BFS data either at BFA or at DRSI only with the express written approval of John James, the BFS System Owner or his designee.</li> </ol> </li> </ol>
<b>3 IT Systems Security</b>		
3.1 IT System Hardening	In place	<ol style="list-style-type: none"> <li>1. BFS operations staff has identified &amp; documented the Solaris 7 &amp; Oracle 9i benchmarks from the Center for Internet Security (CIS) as appropriate hardening levels for the BFS. John James, the BFS System Owner, has approved this recommendation in writing. These benchmarks were most recently applied to BFS in May 2007, &amp; the application was documented in the BFS Change Log.</li> <li>2. BFS operations staff most recently reviewed these benchmarks on June 7, 2007, &amp; determined that they continue to provide an appropriate hardening level for the BFS. Benchmarks are reapplied whenever the operating system or application software is changed.</li> </ol>
	Planned	<ol style="list-style-type: none"> <li>3. PSI, the BFA business partner that operates the BFA technology environment, has engaged Cyberscan, Inc. to conduct a full vulnerability scan of the BFA technology environment. This scan is scheduled for August 2007.</li> <li>4. Based on the results of the vulnerability scan, BFS operations staff will determine whether the CIS benchmarks continue to provide appropriate protection for the BFS.</li> </ol>



# Example Risk Assessment Report

**Table E: Security Controls (continued)**

Control Area	In-Place/ Planned	Description of Controls
<b>4 Logical Access Control</b>		
<b>4.1 Account Management</b>	In place	<p>Documented BFA &amp; BFS policies require:</p> <ol style="list-style-type: none"> <li>1. Granting access to IT system users based on the principle of least privilege. In the case of BFS, however, enforcement of least privilege is accomplished by granting ad-hoc access rights to BFS, rather than granting access based on predefined roles.</li> <li>2. Approval by John James, BFS System Owner &amp; a prospective BFS user's supervisor before granting access to BFS; these policies are enforced.</li> <li>3. Prospective BFS users to receive a BFA-required criminal background check before receiving access to BFS; these policies are enforced.</li> <li>4. The use of passwords on all BFS accounts, &amp; that these passwords expire every 90 days, at a minimum. These policies are not enforced on BFS, however, as passwords are not set to expire &amp; password changes are not enforced.</li> <li>5. Annual review of all BFS accounts to assess the continued need for the accounts &amp; access level. These policies also require automatic locking of accounts if not used for 30 days, disabling of unneeded accounts, retention of account information for 2 years in accordance with BFA records retention policy, &amp; notification of supervisors, Human Resources, &amp; the System Administrator about changes in the need for BFS accounts. These policies are not enforced on BFS, however, &amp; BFS user accounts are not removed when the access is no longer required.</li> <li>6. Prohibit the use of group accounts &amp; shared passwords. These policies are not enforced on BFS, however, as accounts such as "guest," "test," &amp; "share" exist in the BFS user database.</li> <li>7. John James to approve access changes to BFS accounts, &amp; for John James &amp; the BFS operations &amp; support team to investigate unusual account access. These policies are enforced.</li> </ol>
<b>4.2 Password Management</b>	In place	<p>Documented BFA &amp; BFS policies require:</p> <ol style="list-style-type: none"> <li>1. The use of passwords on sensitive systems such as BFS; these policies are enforced on BFS. These policies also require that, at a minimum, passwords be no less than eight characters long &amp; contain both letters &amp; numbers; Windows Active Directory is configured to require this length &amp; complexity for BFS passwords.</li> <li>2. Encryption of passwords during transmission; password encryption, however, is not correctly configured for BFS &amp; BFS passwords are transmitted in clear text.</li> <li>3. Users to maintain exclusive control of their passwords, to allow users to change their passwords at will, &amp; to change a password immediately &amp; notify the ISO if the password is compromised; these policies are enforced.</li> <li>4. BFS users to change passwords every 90 days at a minimum; as noted above, however, these policies are not enforced with respect to BFS.</li> <li>5. The use of password history files to prevent password re-use; these policies are enforced on BFS &amp; BFS retains the previous 240 passwords for each user to prevent their re-use.</li> </ol>

# Example Risk Assessment Report

**Table E: Security Controls (continued)**

Control Area	In-Place/ Planned	Description of Controls
<b>4 Logical Access Control (continued)</b>		
4.2 Password Management (continued)	In place	<p>Documented BFA &amp; BFS policies require:</p> <ol style="list-style-type: none"> <li>7. Use of a procedure for delivery of the initial BFS password in person from the BFS support team in a sealed envelope. The password is expired, &amp; the user is forced to change the password upon first login. Forgotten initial passwords are replaced by the BFS support team &amp; not re-issued.</li> <li>8. Prohibit the use of group accounts &amp; shared passwords. These policies are not enforced on BFS, however, as accounts such as "guest," "test," &amp; "share" exist in the BFS user database.</li> <li>9. Prohibit the inclusion of passwords as plain text in scripts. These policies are not enforced on BFS, however, as passwords are included in scripts &amp; initialization files.</li> <li>10. Limit access to files containing BFS passwords to the BFS support team. These policies are enforced.</li> <li>11. Suppression of passwords on the screen as they are entered. These policies are enforced.</li> <li>12. Members of the BFS support team to have both an administrative &amp; user account &amp; use the administrative account only when performing tasks that require administrative privileges. These policies are enforced.</li> <li>13. At least two members of the BFS support team to have BFS administrative account.</li> </ol>
4.3 Remote Access	In place	<ol style="list-style-type: none"> <li>1. Based on the sensitivity of BFS data, documented BFA &amp; BFS policies require that remote access to BFS not be permitted from outside the PSI-provided third-party network. Remote OS authentication, however, is enabled in the BFS application, even though no user accounts are configured to allow this access.</li> </ol>
	Planned	<ol style="list-style-type: none"> <li>2. To enable alternate work schedules, &amp; work locations, BFA is in the process of developing a plan to allow secure remote access to BFS. This plan is scheduled for completion in October 2007.</li> </ol>
<b>5 Data Protection</b>		
5.1 Data Storage Media Protection	In place	<p>Documented BFA &amp; BFS policies require:</p> <ol style="list-style-type: none"> <li>1. Bea Roberts, as BFS Data Custodian, to provide protection of all sensitive BFS data. These requirements are enforced a written agreement between BFA &amp; Partner Services, Inc.</li> <li>2. Sensitive BFS data not to be stored on mobile data storage media through BFA policy that prohibits local storage of BFS data. This policy is not enforced, however, as sensitive BFS data is stored on USB drives.</li> <li>3. Only authorized DRSI personnel to pickup, receive, transfer, &amp; deliver BFS tapes. This policy is enforced.</li> <li>4. BFS administrators &amp; users to follow the ITRM Removal of Commonwealth Data from Surplus Computer Hard Drives &amp; Electronic Media Standard (ITRM Standard SEC2003-02.1) when disposing of BFS data storage media that are no longer needed. This policy is enforced.</li> <li>5. BFS users to receive training on the proper procedure for disposal of data storage media containing sensitive data as part of the BFA IT Security Awareness &amp; Training program. This policy is enforced.</li> </ol>

# Example Risk Assessment Report

**Table E: Security Controls (continued)**

5 Data Protection (continued)		
5.2 Encryption	In place	<p>BFS uses encryption via:</p> <ol style="list-style-type: none"> <li>1. The secure shell (ssh) &amp; secure copy (scp) protocols, which are in wide commercial use. This use is documented in BFS design documents.</li> <li>2. The CRDSK hard disk encryption product, as documented in BFA &amp; BFS policies.</li> <li>3. Encryption of passwords during transmission. As noted above, however, this feature is incorrectly configured for BFS; BFS passwords are transmitted in clear text.</li> </ol>
	Planned	<ol style="list-style-type: none"> <li>4. BFA is currently documenting Agency policies, standards, &amp; procedures for encryption technologies. Completion of this documentation is planned by October 1, 2007.</li> </ol>
6 Facilities Security		
6.1 Facilities Security	In place	<ol style="list-style-type: none"> <li>1. The BFS is housed in the BFA Data Center with access controlled via a Secure card-key access system, administered by the BFA IRM staff, which permits monitoring, logging, &amp; auditing of all access to the BFA Data Center. Jane Jones, BFA ISO approves all requests for BFA Data Center Access requests based on the principle of least privilege.</li> <li>2. The BFA Data Center is heated &amp; cooled by a 90-ton HVAC unit, separate from the HVAC unit that heats &amp; cools the remainder of the facility. Electric power to the BFA Data Center is provided by four Ribtell 400 Kva units connected to the commercial power supply. Backup power is provided by a diesel-powered generator.</li> <li>3. Fire suppression in the BFA Data Center is provided by a wet-pipe sprinkler system. BFA is aware that this fire suppression system poses a risk of significant water damage to equipment in the data center, including BFS. Replacement of the wet-pipe sprinkler system, however, has been considered &amp; is cost-prohibitive.</li> <li>4. Access to the BFA facility at 123 Elm St. is also protected by the Secure card-key access system, administered by the BFA IRM staff. Cards that permit access to the facility are given only to BFA employees &amp; contractors upon supervisory approval. All visitors are required to have escorts in the BFA facility.</li> <li>5. Access to other areas in the BFA facility that house IT resources is controlled via means of cipher locks, also administered by the BFA IRM staff, which changes the lock ciphers every 90 days. Jane Jones, BFA ISO approves all requests for access to the lock cipher based on the rule of least privilege.</li> </ol>

# Example Risk Assessment Report

**Table E: Security Controls (continued)**

7 Personnel Security		
7.1 Access Determination & Control	In place	<ol style="list-style-type: none"> <li>1. BFS users receive a BFA-required fingerprint criminal background check &amp; a credit check before receiving access to BFS.</li> <li>2. Access to the BFA facility &amp; the BFA Data Center that houses the BFS is controlled by card-key access.</li> <li>3. Adequate separation of duties exists for BFS in order to guard against the possibility of fraud.</li> </ol> <p>Documented BFA &amp; BFS policies require:</p> <ol style="list-style-type: none"> <li>4. The removal of physical &amp; logical access rights upon transfer or termination of staff or when the need for access no longer exists. These policies are enforced with respect to physical access; as noted above, they are not enforced regarding logical access to BFS.</li> <li>5. Return of Agency assets upon transfer or termination. These policies are enforced.</li> <li>6. Granting access to IT system users based on the principle of least privilege. These policies are enforced with respect to physical access. In the case of BFS, however, enforcement of least privilege is accomplished by granting ad-hoc access rights to BFS, rather than granting access based on predefined roles.</li> </ol>
7.2 IT Security Awareness & Training	In place	<ol style="list-style-type: none"> <li>1. Jane Jones, BFA ISO, is responsible for BFA's IT security awareness &amp; training program. BFA requires, through documented policies &amp; procedures, that all employees &amp; contractors complete an on-line IT security training program on an annual basis. The online training program, which has been customized by the vendor to BFA's specifications, both records completion &amp; forwards records of completion to the BFA ISO. The online training program covers:               <ol style="list-style-type: none"> <li>a. BFA policies for protecting IT systems &amp; data, with a particular emphasis on sensitive systems &amp; data;</li> <li>b. The concept of separation of duties;</li> <li>c. Employee responsibilities in continuity of operations, configuration management, &amp; incident detection &amp; reporting;</li> <li>d. IT system user responsibilities &amp; best practices in:                   <ol style="list-style-type: none"> <li>1. Prevention, detection, &amp; eradication of malicious code;</li> <li>2. Proper disposal of data storage media; &amp;</li> <li>3. Proper use of encryption products;</li> </ol> </li> <li>e. Access controls, including creating &amp; changing passwords &amp; the need to keep them confidential;</li> <li>f. BFA Remote Access policies; &amp;</li> <li>g. Intellectual property rights, including software licensing &amp; copyright issues.</li> </ol> </li> <li>2. BFA employees &amp; contractors are required to accept BFA IT security policies by completing an online agreement during the online IT security training.</li> <li>3. Members of the BFS support team, BFA DR &amp; Incident Response (IR) team members, &amp; IRM staff are required to complete the equivalent of 40 contact hours or 3.0 CEUs of specialized IT security training related to their roles, though documented BFA policy, which is enforced.</li> <li>4. BFA policy requires that all employees &amp; contractors complete required basic IT security training within two weeks of beginning work at BFA; this policy is enforced.</li> </ol>

# Example Risk Assessment Report

Table E: Security Controls (continued)		
<b>7 Personnel Security (continued)</b>		
7.3 Acceptable Use	In place	1. BFA has elected to use the Virginia Department of Human Resource Management Policy 1.75 – Use of Internet & Electronic Communication Systems as its Acceptable Use policy. BFA employees & contractors are required to agree to this policy by completing an online agreement at the conclusion of online IT security training.
	Planned	2. BFA is in the process of developing its own Acceptable Use policy. Completion is expected in December 2007.
<b>8 Threat Management</b>		
8.1 Threat Detection	In place	<p>Jane Jones, BFA ISO is responsible for BFA's threat detection program, which includes the following components:</p> <ol style="list-style-type: none"> <li>1. BFA IRM staff receive threat detection training annually as their advanced IT security training.</li> <li>2. PSI has deployed &amp; monitors Intrusion Detection Systems (IDS) &amp; Intrusion Prevention Systems (IPS) are in the BFA environment.</li> <li>3. PSI security staff maintains regular communication with US-CERT &amp; other security research &amp; coordination organizations, review IDS &amp; IPS logs in real-time, &amp; recommend appropriate measures to BFA.</li> </ol>
8.2 Incident Handling	In place	<p>BFA has documented &amp; enforces:</p> <ol style="list-style-type: none"> <li>1. An Incident Response Team that includes the BFA ISO, BFA IRM staff, &amp; PSI support &amp; security staff.</li> <li>2. A protocol to use IT Security Audits, Risk Assessments, &amp; post-incident review to identify appropriate measures to defend against &amp; respond to cyber attacks.</li> <li>3. Proactive measures to prevent cyber attacks in response to recommendations from the PSI security staff.</li> <li>4. Internal BFA incident investigation, reporting, &amp; recording processes.</li> </ol> <p>PSI has documented &amp; enforces on BFA's behalf:</p> <ol style="list-style-type: none"> <li>5. Proactive measures to prevent cyber attacks in response to recommendations from the PSI security staff.</li> <li>6. Incident categorization &amp; prioritization criteria, along with procedures to respond to each level of attack.</li> <li>7. A reporting process for reporting IT security incidents in accordance with §2.2-603(F) of the Code of Virginia, including reporting IT security incidents only through channels that have not been compromised.</li> </ol>
8.3 Security Monitoring & Logging	In place	<p>BFA has documented designation of PSI security staff as responsible for:</p> <ol style="list-style-type: none"> <li>1. Development of logging capabilities &amp; review procedures for BFA as a whole, as well as for the BFS.</li> <li>2. Enabling logging on all BFS components &amp; retention of logs for 90 days.</li> <li>3. Monitoring BFS security logs in real time &amp; alerts the BFS support team &amp; BFA IRM staff by pager when suspicious activity occurs.</li> </ol>

# Example Risk Assessment Report

**Table E: Security Controls (continued)**

9 IT Asset Management		
9.1 IT Asset Control	In place	<p>Documented &amp; enforced BFA &amp; BFS policies require:</p> <ol style="list-style-type: none"> <li>1. No BFA IT assets to be removed from BFA premises, except for laptop computers assigned to individual BFA employees.</li> <li>2. No IT assets not owned by BFA to be connected to any BFA system or network.</li> <li>3. Removal of data from BFA IT assets prior to disposal in accordance with the COV Removal of Commonwealth Data from Surplus Computer Hard Drives &amp; Electronic Media Standard (ITRM Standard SEC2003-02.1).</li> </ol>
9.2 Software License Management	In place	<ol style="list-style-type: none"> <li>1. Documented BFA policies require the use of only BFA-approved software on its IT systems &amp; require annual reviews of whether all software is used in accordance with license requirements.</li> <li>2. All BFS software is appropriately licensed.</li> </ol>
9.3 Configuration Management & Change Control	In place	<ol style="list-style-type: none"> <li>1. BFA has document configuration management &amp; change control policies adequate so that changes to the IT environment do not introduce additional IT security risk. BFA enforces these policies with respect to the BFS.</li> </ol>

# Example Risk Assessment Report

Identify the security controls for each risk identified in Table D above. Associate the risks with the relevant controls in a Risks-Controls table (Table F), as below. This correlation determines whether controls exist that respond adequately to the identified risks. Indicate where controls are not in place or where they appear not to have been implemented effectively. Also indicate any factors that mitigate or exacerbate the absence of effective controls.

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

<b>Table F: Risks-Controls-Factors Correlation</b>		
<b>Risk No.</b>	<b>Risk Summary</b>	<b>Correlation of Relevant Controls &amp; Other Factors</b>
1	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.	There are no controls relevant to this risk; neither are there any mitigating or exacerbating factors. BFA Executive Management has accepted this risk.
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.	Controls 4.1.5 and 7.1.4 are in place for closing unneeded and unused user accounts, but are not enforced.  A mitigating factor is that the risk depends on a gaining access to the client application. Physical access to the building, workstation areas, & network are adequately protected.
3	Unauthorized access via ad-hoc privileges could compromise confidentiality & integrity of BFS data.	Controls 4.1.1 and 7.1.6 require users to receive the minimum access rights needed to perform job functions. These controls are in place on an ad-hoc basis rather than based on roles, as required by policy.
4	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.	Control 8.2.1 provides intrusion detection sufficient to detect such an attack. No Intrusion Prevention System (IPS) is in place, however, to prevent such an attack.
5	Exploitation of unpatched application security flaws could compromise confidentiality & integrity of BFS data.	Control 8.1.3 requires that advisories & critical patch releases should be monitored. These procedures are not followed consistently. A mitigating factor is that occurrence of the risk depends on gaining access to the internal Agency network. A BFA firewall protects the Internet connection & a Data Center firewall protects the Data Center network. In addition, dial-in access is limited & strictly controlled. Internal users still pose a significant threat.

# Example Risk Assessment Report

**Table F: Risks-Controls Correlation (continued)**

Risk No.	Risk	Analysis of Relevant Controls & Other Factors
6	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.	Control 4.2.9 requires that clear text passwords must not exist in scripts or text files on any system, but is not enforced for BFS. The use of clear text passwords is an inherent weakness in the client software, & there is no fix according to the vendor. Physical protections are in place to limit access to the building & user workstation areas, & technical controls are in place to limit access to user workstations to those individuals who have been granted permission to logon to Agency systems.
7	Compromise of unexpired/unchanged passwords could result in compromise of confidentiality & integrity of BFS data.	Controls 4.1.4 and 4.2.4 require regular password changes, but are not enforced for BFS. Support for required password changes is built into the software but have not been enabled.
8	Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data.	Controls 4.1.6 and 4.2.8 require that shared accounts such as these not be used but have not enforced for BFS.
9	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	Control 4.3.1 prohibits access to BFS from outside the PSI third-party network; enabling remote access in the software violates this control. A mitigating factor is that only authorized users could access the application. This mitigating effect of this factor is reduced by the unused accounts that continue to exist on BFS.
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.	Controls 4.2.9 and 4.5.3 require encryption of passwords, but have not been enforced for BFS. Physical security protections are in place that would limit the ability to sniff the network to exploit this vulnerability.
11	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.	Control 4.4.2 prohibits storage of sensitive BFS data on portable media such as USB drives, but has not been enforced for BFS.

After preparing the table, enter the controls data in Exhibit 1 (this data entry can be accomplished by cutting and pasting from Table F).

# Example Risk Assessment Report

## 5 RISK LIKELIHOOD DETERMINATION

The purpose of this step is to assign a likelihood rating of high, moderate or low to each risk identified in Table D. This rating is a subjective judgment based on the likelihood a vulnerability might be exploited by a credible threat. The following factors should be considered:

- Threat-source motivation and capability, in the case of human threats;
- Probability of the threat occurring, based on statistical data or previous experience, in the case of natural and environmental threats; and
- Existence and effectiveness of current or planned controls

### 5 Risk Likelihood Determination

Table G defines the Risk Likelihood ratings for the BFS.

*Other factors may also be used to estimate likelihood. These include historical information, records and information from security organizations such as US-CERT and other sources. The controls listed in Table E may be considered, provided they adequately mitigate the risk. Agencies are strongly encouraged to use risk likelihood definitions of high, moderate, and low, as documented in Table G.*

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
High	Low	Low	Moderate
Moderate	Low	Moderate	High
Low	Moderate	High	High

Table H, which begins on the next page, 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 G, to each BFS risk documented in Table D.

# Example Risk Assessment Report

<b>Table H: Risk Likelihood Ratings</b>			
<b>Risk No.</b>	<b>Risk Summary</b>	<b>Risk Likelihood Evaluation</b>	<b>Risk Likelihood Rating</b>
1	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.	There are no controls against water damage to BFS from the wet-pipe sprinkler system in the event of a fire, so the effectiveness of controls is low. The likelihood of fire in the BFA Data Center is low.	Moderate
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.	Effectiveness of controls for closing user accounts is low, as unneeded user IDs exist on BFS. Threat source capability is also low as the risk is dependent on learning a user ID & password & gaining access to the client application. There appear to be adequate protections against this risk. Physical access to the building, workstation areas, & network are adequately protected.	Moderate
3	Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of BFS data.	Effectiveness of controls to limit users to minimum access rights is moderate. Policies now in place enable these controls but on an ad-hoc basis rather than based on roles, as required by policy. Threat source capability and motivation is rated moderate as only authorized users could cause this risk.	Moderate
4	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.	No controls are in place to prevent such an attack, so control effectiveness is low. Threat source capability and motivation is rated moderate as reward from attacking BFS in this manner is limited.	Moderate
5	Exploitation of unpatched application security flaws could compromise confidentiality & integrity of BFS data.	Effectiveness of controls to require timely application of patches to BFS is low as procedures for applying such patches are not followed consistently. Threat source motivation and capability is rated as low as occurrence of the risk depends on an unauthorized user's gaining access to the internal Agency network. There is an Agency firewall protecting the Internet connection & a Data Center firewall protecting the Data Center network. Additionally, dial-in access is limited & strictly controlled.	Moderate

# Example Risk Assessment Report

**Table H: Risk Likelihood Ratings (continued)**

Risk No.	Risk Summary	Risk Likelihood Evaluation	Risk Likelihood Rating
6	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.	Effectiveness of controls prohibiting use of clear text passwords in scripts or text files is low as the use of clear text passwords is an inherent weakness in the client software. Threat source capability is rated low, as physical protections are in place to limit access to the building & user workstation areas, & technical controls are in place to limit access to user workstations to those individuals who have been granted permission to logon to Agency systems.	Moderate
7	Compromise of unexpired/unchanged passwords could result in compromise of confidentiality & integrity of BFS data.	Effectiveness of controls requiring regular password changes is low; these changes are not required. Threat source capability is rated low as the risk depends on learning a user ID & password & gaining access to the client application.	Moderate
8	Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data.	Effectiveness of controls that prohibit shared accounts such as these is low. Threat capability is high as user IDs for generic accounts such as these are well-known.	High
9	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	Effectiveness of controls requiring that remote access is enabled only where authorized and required is low, as these controls have not been followed. Threat source capability is moderate because of the unused accounts that exist on BFS.	High
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.	Effectiveness of controls requiring encryption of passwords is low, as these controls have not been followed. Threat source capability is low as physical security protections are in place that would limit the ability to sniff the network to exploit this vulnerability.	Moderate
11	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.	Effectiveness of controls prohibiting storage of sensitive data on USB drives is low, as these controls have not been followed. Threat source capability is high as such USB drives are frequently lost or stolen.	High

# Example Risk Assessment Report

## 6 RISK IMPACT ANALYSIS

The purpose of this step is to assign an impact rating of high, moderate or low to each risk identified in Table D. The impact rating is determined based on the severity of the adverse impact that would result from an occurrence of the risk. Agencies are urged to assign ratings based on the impact to the COV as a whole.

### 6 Risk Impact Analysis

**Table I documents the ratings used to evaluate the impact of BFS risks on the COV and BFA.**

Table I provides definitions of the impact ratings that agencies are strongly encouraged to use. Include the impact ratings used in the Risk Assessment Report.

<b>Table I: Risk Impact Rating Definitions</b>	
<b>Magnitude of Impact</b>	<b>Impact Definition</b>
<b>High</b>	<b>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.</b>
<b>Moderate</b>	<b>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.</b>
<b>Low</b>	<b>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</b>

*When determining the impact rating the following governing factors should be considered:*

- *The business process performed by the IT system.*
- *System and data sensitivity (i.e., the level of protection required to maintain system and data integrity, confidentiality, and availability).*

*Impact can also be based on ability to provide service to the public. An adverse impact might be a loss of confidentiality, integrity, or availability, or a loss of public trust in COV. Factors to consider are the loss or inconvenience the public would suffer if the risk were to occur. This information can usually be obtained from the Agency's Business Impact Analysis (BIA).*

Apply the impact definitions in Table H to the risks identified in Table D to evaluate the effect if the risk occurs.

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

# Example Risk Assessment Report

**Table J: Risk Impact Analysis**

Risk No.	Risk Summary	Risk Impact	Risk Impact Rating
1	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.	BFS unavailable for use.	High
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.	Unauthorized disclosure or modification of BFS data.	High
3	Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of BFS data.	Unauthorized disclosure or modification of BFS data.	High
4	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.	BFS unavailable for use	High
5	Exploitation of un-patched application security flaws could compromise confidentiality & integrity of BFS data.	Unauthorized disclosure or modification of BFS data.	High
6	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.	Unauthorized disclosure or modification of BFS data.	High
7	Compromise of unexpired/ unchanged passwords could result in compromise of confidentiality & integrity of BFS data.	Unauthorized disclosure or modification of BFS data.	High
8	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	Unauthorized disclosure or modification of BFS data.	High
9	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	Unauthorized disclosure or modification of BFS data.	High
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.	Unauthorized disclosure or modification of BFS data.	High
11	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.	Unauthorized disclosure of BFS data.	High

# Example Risk Assessment Report

Assign an impact rating to each risk identified in Table D. Enter the data in Exhibit A. This data entry can be accomplished by cutting and pasting from Table I.

**This section contains the results of an impact analysis performed for the BFS. To perform this analysis, an impact rating of low, moderate, or high was assigned to each risk identified in Table D. The impact rating for each risk was determined based on the severity of the adverse impact that would result from a successful exploitation of the vulnerability. The impact ratings in this section for each individual risk were based on the system's mission, and system and data sensitivity. BFA's most recent Business Impact Analysis (BIA) was reviewed in determining the ratings.**

# Example Risk Assessment Report

## 7 OVERALL RISK DETERMINATION

The purpose of this step is to calculate an overall risk rating of high, moderate or low for each risk identified in Table D. The risk rating must be based on both the likelihood of the risk occurring and on the impact to the COV should the risk occur.

### 7 Overall Risk Determination

*The determination of risk ratings is somewhat subjective. Their value is in the attempt to quantify, however subjectively, the combination of likelihood and impact of occurrence. Each risk rating is expressed as the correlation of the given risk's likelihood of occurrence, and the risk's respective impact rating. The resulting risk ratings will place the various risk on a scale (e.g., 1 to 100), thus enabling managers to rank the risks quantitatively in order of severity and priority.*

*For example:*

- *Each risk likelihood rating assigned in Table H, may be assigned a numerical value of 0.1 for low, 0.5 for moderate, or 1.0 for high to represent the probability of occurrence (i.e., 0.1 to 1.0).*
- *Each risk impact rating assigned Table I, may be assigned a numerical value of 10 for low, 50 for moderate, or 100 for high to represent a quantified impact estimate (i.e., 10 to 100).*
- *Calculate the overall risk ratings for each risk by multiplying the numerical ratings assigned for likelihood and impact.*

*For a thorough description of the risk rating calculation, refer to the annotated NIST SP 800-30, Table 3-6, "Risk Scale and Necessary Actions."*

Table J, taken from NIST SP 800-30, is an example of a risk-rating matrix showing how the overall risk ratings for a 3x3 matrix (i.e., high, moderate and low likelihood by low, moderate and high impact) are to be derived. If your agency requires more granular risk ratings, a larger matrix (e.g., 4x4, 3x5) may be used.

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

# Example Risk Assessment Report

Table K: Overall Risk Rating Matrix			
Risk Likelihood	Risk Impact		
	Low (10)	Moderate (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Moderate $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Moderate (0.5)	Low $10 \times 0.5 = 5$	Moderate $50 \times 0.5 = 25$	Moderate $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

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

Assign a risk rating to each risk listed in Table D. Enter the risk ratings in Exhibit A. This data entry can be accomplished by cutting and pasting from Table K.

Table L assigns risk ratings from Table K to the risks identified for the BFS.

Table L: Overall Risk Ratings Table				
Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
1	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.	Moderate	High	Moderate
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.	Moderate	High	Moderate
3	Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of BFS data.	Moderate	High	Moderate
4	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.	Moderate	High	Moderate
5	Exploitation of un-patched application security flaws could compromise confidentiality & integrity of BFS data.	Moderate	High	Moderate
6	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.	Moderate	High	Moderate

# Example Risk Assessment Report

**Table L: Risk Ratings Table (continued)**

Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
7	Compromise of unexpired/unchanged passwords could result in compromise of confidentiality & integrity of BFS data.	Moderate	High	Moderate
8	Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data.	High	High	High
9	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	High	High	High
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.	Moderate	High	Moderate
11	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.	High	High	High

Describe the process used in assigning overall risk ratings.

This section contains the results of a risk determination performed for the Budget Formulation System. A risk rating of low, moderate, or high was assigned to each risk identified in Table D. The risk rating for each individual risk was calculated using guidance provided in NIST SP 800-30, Table 3-6, "Risk Scale and Necessary Actions."

# Example Risk Assessment Report

## 8 RECOMMENDATIONS

The purpose of this step is to recommend additional actions required to respond to the identified risks, as appropriate to the agency's operations. The goal of the recommended risk response is to reduce the residual risk to the system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

### 8 Recommendations

Table M documents recommendations for the risks identified for the BFS system.

**Table M: Recommendations**

Risk No.	Risk Summary	Risk Rating	Recommendations
1	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.	Moderate	None. Replacing the wet-pipe sprinkler system in the BFA Data Center has been determined to be cost-prohibitive. BFA executive management has elected to accept this risk.
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.	Moderate	The BFS support team should follow BFA & BFS policies regarding removal of accounts. BFA IRM should develop & implement a process to verify that termination procedures are carried out in the timeframe specified by BFA & BFS policy.
3	Unauthorized access via ad-hoc privileges could compromise confidentiality & integrity of BFS data.	Moderate	BFA IRM should develop BFS user roles & associated privileges. Once developed the BFS support team should implement these roles & assign BFS privileges based on role.
4	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.	High	BFA IRM staff and the PSI support team should analyze whether replacing the existing Intrusion Detection Systems (IDS) with an Intrusion Prevention System is a cost-effective response to this risk.

# Example Risk Assessment Report

**Table M: Recommendations (continued)**

Risk No.	Risk Summary	Risk Rating	Recommendations
5	Exploitation of unpatched application security flaws could compromise confidentiality & integrity of BFS data.	Moderate	The BFS support team should implement procedures for reviewing & updating vendor-recommended patches so that patches ensure are applied in a timely manner. An automated notification process should be developed to notify the appropriate individuals of critical updates.
6	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.	Moderate	The client software should be rewritten so that clear-text user IDs & passwords are not used in script and initialization files.
7	Compromise of unexpired/unchange d passwords could result in compromise of confidentiality & integrity of BFS data.	Moderate	The BFS support team should enable the functionality within Oracle to expire passwords & require changes.
8	Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data.	High	The BFS support team should remove all generic accounts from BFS. BFA IRM should monitor accounts should continue to verify that no new shared accounts are created.
9	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	High	As an immediate step, the BFS support team should disable the remote OS feature. As documented in planned controls, the BFA IRM staff and BFS support team should work to develop a secure method to allow remote access to BFS.
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.	Moderate	The BFS support team should configure the login encryption feature properly.
11	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.	High	BFA should include the prohibition on storing sensitive data on removable media such as USB drives in the BFA Acceptable Use policy, under development, and in the BFA Security Awareness and Training program.

# Example Risk Assessment Report

Develop a list of recommendations related to the risks in Table D. Enter the recommendations into Exhibit 1. This data entry can be accomplished by cutting and pasting from Table M.

# Example Risk Assessment Report

## 9 RESULTS DOCUMENTATION

The final step in the risk assessment is to complete the Risk Assessment Matrix located in Exhibit 1. The data gathered in the previous steps should be used to populate the matrix. Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed and controls assessed and recommended), the results should be documented in an official report or management brief.

The Risk Assessment Matrix located in Exhibit 1 serves as the basis for preparing the official report or management brief and documenting the risk assessment results. The risk assessment report helps senior management, the mission owners, makes informed decisions on policy, procedural, budget and system operational and management changes. A risk assessment is not an audit or investigation report, which often looks for wrongdoing and issues findings that can be embarrassing to managers and system owners. A risk assessment is a systematic, analytical tool for identifying security weaknesses and calculating risk. The risk assessment report should not be presented in an accusatory manner. It should rather be a frank and open discussion of the observations of the risk assessment team. Its purpose is to inform senior management of the current threat-vulnerability environment and the adequacy of current and planned security controls. The value of a risk assessment is that it helps senior management to understand the current system exposure so they can allocate resources effectively and efficiently to correct errors and reduce potential losses.

*The analysis should assess the effectiveness of in-place or planned controls in responding to the identified risks to the system. Compliance with these controls should be evaluated on an annual basis through a security self-assessment.*

*Other considerations, which are beyond the scope of the risk assessment but which may be addressed in the report and should be discussed in the brief, are management's assessment and subsequent corrective action plan (CAP) to address the identified weaknesses. For each recommendation management should:*

- *Assign a priority to the recommendation;*
- *Assign responsibility to an individual or identify the department that will be held accountable for implementing the recommendation;*
- *Provide a date for initiating the recommendation; and*
- *Provide a date by which time the recommendations must be fully implemented.*

Complete the Risk Assessment Matrix in Exhibit 1 (much of the required data entry can be accomplished by cutting and pasting data from the Tables developed throughout the process). Prepare an official report or management brief to explain the results of the risk assessment and provide the rationale for the recommended security controls.

**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	Wet-pipe sprinkler system in BFS Data Center.	Fire	Compromise of BFS availability.	Fire would activate sprinkler system causing water damage & compromising the availability of BFS.	Moderate	High	Moderate	There are no controls relevant to this risk; neither are there any mitigating or exacerbating factors.	None. Replacing the wet-pipe sprinkler system in the BFA Data Center has been determined to be cost-prohibitive. BFA executive management has elected to accept this risk.
2	BFS user identifiers (IDs) no longer required are not removed from BFS in timely manner.	Unauthorized Use	Compromise of confidentiality & integrity of BFS data.	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of BFS data.	Moderate	High	Moderate	Controls 4.1.5 and 7.1.4 are in place for closing unneeded and unused user accounts, but are not enforced.  A mitigating factor is that the risk depends on a gaining access to the client application. Physical access to the building, workstation areas, & network are adequately protected.	The BFS support team should follow BFA & BFS policies regarding removal of accounts.  BFA IRM should develop & implement a process to verify that termination procedures are carried out in the timeframe specified by BFA & BFS policy.
3	BFS access privileges are granted on an ad-hoc basis rather than predefined roles.	Unauthorized Access	Compromise of confidentiality & integrity of BFS data.	Unauthorized access via ad-hoc privileges could compromise confidentiality & integrity of BFS data.	Moderate	High	Moderate	Controls 4.1.1 and 7.1.6 require users to receive the minimum access rights needed to perform job functions. These controls are in place on an ad-hoc basis rather than based on roles, as required by policy.	BFA IRM should develop BFS user roles & associated privileges. Once developed the BFS support team <i>should</i> implement these roles & assign BFS privileges based on role.

Exhibit 1: Risk Assessment Matrix (continued)									
Risk No.	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls and Other Factors	Recommendations
4	Bogus TCP packets (> 50000 bytes) directed at port 1521 will cause BFS to stop responding.	Malicious Use Computer Crime	Compromise of BFS availability.	Denial of service attack via large bogus packets sent to port 1521 could render BFS unavailable for use.	Moderate	High	Moderate	Control 8.2.1 provides intrusion detection sufficient to detect such an attack. No Intrusion Prevention System (IPS) is in place to prevent such an attack, however.	BFA IRM staff and the PSI support team should analyze whether replacing the existing Intrusion Detection Systems (IDS) with an Intrusion Prevention System is a cost-effective response to this risk.
5	New patches exist to correct flaws in application security design have not been applied.	Malicious Use Computer Crime	Compromise of confidentiality & integrity of BFS data.	Exploitation of un-patched application security flaws could compromise confidentiality & integrity of BFS data.	Moderate	High	Moderate	Control 8.1.3 requires that advisories & critical patch releases should be monitored. These procedures are not followed consistently. A mitigating factor to consider is that occurrence of the risk depends on an unauthorized user's gaining access to the internal Agency network. There is an Agency firewall protecting the Internet connection & a Data Center firewall protecting the Data Center network. In addition, dial-in access is limited & strictly controlled. Internal users still pose a significant threat.	The BFS support team should implement procedures for reviewing & updating vendor-recommended patches so that patches ensure are applied in a timely manner.  An automated notification process should be developed to notify the appropriate individuals of critical updates.

**Exhibit 1: Risk Assessment Matrix (continued)**

Risk No.	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls and Other Factors	Recommendations
6	User names & passwords are in scripts & initialization files.	Malicious Use Computer Crime	Compromise of confidentiality & integrity of BFS data.	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of BFS data.	Moderate	High	Moderate	Control 4.2.9 requires that clear text passwords must not exist in scripts or text files on any system, but is not enforced for BFS. The use of clear text passwords is an inherent weakness in the client software, & there is no fix according to the vendor. Physical protections are in place to limit access to the building & user workstation areas, & technical controls are in place to limit access to user workstations to those individuals who have been granted permission to logon to Agency systems.	The client software should be rewritten so that clear-text user IDs & passwords are not used in script and initialization files.
7	Passwords are not set to expire; regular password changes are not enforced.	Malicious Use Computer Crime	Compromise of confidentiality & integrity of BFS data.	Compromise of unexpired/ unchanged passwords could result in compromise of confidentiality & integrity of BFS data.	Moderate	High	Moderate	Controls 4.1.4 and 4.2.4 require regular password changes, but are not enforced for BFS. Support for required password changes is built into the software but have not been enabled.	The BFS support team should enable the functionality within Oracle to expire passwords & require changes.
8	“Generic” accounts found in the database (e.g., test, share, guest).	Malicious Use Computer Crime	Compromise of confidentiality & integrity of BFS data.	Use of generic BFS accounts could result in compromise of confidentiality & integrity of sensitive BFS data.	High	High	High	Controls 4.1.6 and 4.2.8 require that shared accounts such as these not be used but have not enforced for BFS.	The BFS support team should remove all generic accounts from BFS. BFA IRM should monitor accounts should continue to verify that no new shared accounts are

**Exhibit 1: Risk Assessment Matrix (continued)**

Risk No.	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls and Other Factors	Recommendations
9	Remote OS authentication is enabled but not used.	Malicious Use Computer Crime	Compromise of confidentiality & integrity of BFS data.	Remote access is not currently used by BFS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive BFS data.	High	High	High	Control 4.3.1 prohibits access to BFS from outside the PSI third-party network; enabling remote access in the software violates this control. A mitigating factor is that only authorized users could access the application. This mitigating effect of this factor is reduced by the unused accounts that continue to exist on BFS.	As an immediate step, the BFS support team should disable the remote OS feature. As documented in planned controls, the BFA IRM staff and BFS support team should work to develop a secure method to allow remote access to BFS.
10	Login encryption setting is not properly configured.	Malicious Use Computer Crime	Compromise of confidentiality & integrity of BFS data.	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive BFS data.	Moderate	High	Moderate	Controls 4.2.9 and 4.5.3 require encryption of passwords, but have not been enforced for BFS. Physical security protections are in place that would limit the ability to sniff the network to exploit this vulnerability.	The BFS support team should configure the login encryption feature properly.
11	Sensitive BFS data is stored on USB drives	Malicious Use Computer Crime	Compromise of confidentiality of BFS data.	Loss or theft of USB drives could result in compromise of confidentiality of BFS data.	High	High	High	Control 4.4.2 prohibits storage of sensitive BFS data on portable media such as USB drives, but has not been enforced for BFS.	BFA should include the prohibition on storing sensitive data on removable media such as USB drives in the BFA Acceptable Use policy, under development, and in the BFA Security Awareness and Training program.

**RISK ASSESSMENT REPORT TEMPLATE**

**Information Technology Risk Assessment  
For**

Risk Assessment Report

*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

1	INTRODUCTION .....	1
2	IT SYSTEM CHARACTERIZATION .....	37
3	RISK IDENTIFICATION.....	4
4	CONTROL ANALYSIS .....	6
5	RISK LIKELIHOOD DETERMINATION .....	9
6	RISK IMPACT ANALYSIS.....	11
7	OVERALL RISK DETERMINATION .....	37
8	RECOMMENDATIONS .....	37
9	RESULTS DOCUMENTATION .....	37

## LIST OF EXHIBITS

EXHIBIT 1: RISK ASSESSMENT MATRIX.....	37
--	----

## LIST OF FIGURES

FIGURE 1 – IT SYSTEM BOUNDARY DIAGRAM.....	3
FIGURE 2 – INFORMATION FLOW DIAGRAM.....	3

## LIST OF TABLES

TABLE A: RISK CLASSIFICATIONS .....	37
TABLE B: IT SYSTEM INVENTORY AND DEFINITION.....	2
TABLE C: THREATS IDENTIFIED .....	4
TABLE D: VULNERABILITIES, THREATS, AND RISKS .....	5
TABLE E: SECURITY CONTROLS .....	6
TABLE F: RISKS-CONTROLS-FACTORS CORRELATION .....	8
TABLE G: RISK LIKELIHOOD DEFINITIONS.....	9
TABLE H: RISK LIKELIHOOD RATINGS.....	9
TABLE I: RISK IMPACT RATING DEFINITIONS.....	37
TABLE J: RISK IMPACT ANALYSIS .....	37
TABLE K: OVERALL RISK RATING MATRIX.....	37
TABLE L: OVERALL RISK RATINGS TABLE .....	37
TABLE M: RECOMMENDATIONS .....	37

# 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

Table B: IT System Inventory and Definition				
<b>IT System Inventory and Definition Document</b>				
<b>I. IT System Identification and Ownership</b>				
<b>IT System ID</b>		<b>IT System Common Name</b>		
<b>Owned By</b>				
<b>Physical Location</b>				
<b>Major Business Function</b>				
<b>System Owner Phone Number</b>		<b>System Administrator(s) Phone Number</b>		
<b>Data Owner(s) Phone Number(s)</b>		<b>Data Custodian(s) Phone Number(s)</b>		
<b>Other Relevant Information</b>				
<b>II. IT System Boundary and Components</b>				
<b>IT System Description and Components</b>				
<b>IT System Interfaces</b>				
<b>IT System Boundary</b>				
<b>III. IT System Interconnections (add additional lines, as needed)</b>				
<b>Agency or Organization</b>	<b>IT System Name</b>	<b>IT System ID</b>	<b>IT System Owner</b>	<b>Interconnection Security Agreement Status</b>
<b>IV. IT System and Data Sensitivity (add additional lines, as needed)</b>				
<b>Type of Data</b>	<b>Sensitivity Ratings</b>			
	<b>Include Rationale for each Rating</b>			
	<b>Confidentiality</b>	<b>Integrity</b>	<b>Availability</b>	
<b>Overall IT System Sensitivity</b>	<b>Overall IT System Sensitivity Rating</b>			
	Must be "high" if sensitivity of any data type is rated "high" on any criterion			
	<input type="checkbox"/> <b>HIGH</b>	<input type="checkbox"/> <b>MODERATE</b>	<input type="checkbox"/> <b>LOW</b>	

Risk Assessment Report

<b>Rating and Classification</b>	<b>IT System Classification</b> Must be "Sensitive" if overall sensitivity is "high"; consider as "Sensitive" if overall sensitivity is "moderate"
	<input type="checkbox"/> <b>SENSITIVE</b> <span style="float: right;"><input type="checkbox"/> <b>NON-SENSITIVE</b></span>

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***

## Risk Assessment Report

### 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.

Risk Assessment Report

**Table D: Vulnerabilities, Threats, and Risks**

<b>Risk No.</b>	<b>Vulnerability</b>	<b>Threat</b>	<b>Risk of Compromise of</b>	<b>Risk Summary</b>
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.

<b>Table E: Security Controls</b>		
<b>Control Area</b>	<b>In-Place/ Planned</b>	<b>Description of Controls</b>
<b>1 Risk Management</b>		
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		
<b>2 IT Contingency Planning</b>		
2.1 Continuity of Operations Planning		
2.2 IT Disaster Recovery Planning		
2.3 IT System & Data Backup & Restoration		
<b>3 IT Systems Security</b>		
3.1 IT System Hardening		
3.2 IT Systems Interoperability Security		
3.3 Malicious Code Protection		
3.4 IT Systems Development Life Cycle Security		
<b>4 Logical Access Control</b>		

Risk Assessment Report

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

Risk Assessment Report

<b>Risk No.</b>	<b>Risk Summary</b>	<b>Risk Likelihood Evaluation</b>	<b>Risk Likelihood Rating</b>
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

## 6 IMPACT ANALYSIS

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

<b>Table I: Risk Impact Rating Definitions</b>	
<b>Magnitude of Impact</b>	<b>Impact Definition</b>
<b>High</b>	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.
<b>Moderate</b>	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.
<b>Low</b>	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.

<b>Table J: Risk Impact Analysis</b>			
<b>Risk No.</b>	<b>Risk Summary</b>	<b>Risk Impact</b>	<b>Risk Impact Rating</b>
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Risk Assessment Report

<b>Risk No.</b>	<b>Risk Summary</b>	<b>Risk Impact</b>	<b>Risk Impact Rating</b>
16			
17			
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 $10 \times 1.0 = 10$	Moderate $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Moderate (0.5)	Low $10 \times 0.5 = 5$	Moderate $50 \times 0.5 = 25$	Moderate $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

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				

Risk Assessment Report

<b>Risk No.</b>	<b>Risk Summary</b>	<b>Risk Likelihood Rating</b>	<b>Risk Impact Rating</b>	<b>Overall Risk Rating</b>
19				
20				
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.

<b>Table M: Recommendations</b>			
<b>Risk No.</b>	<b>Risk</b>	<b>Risk Rating</b>	<b>Recommendations</b>
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									