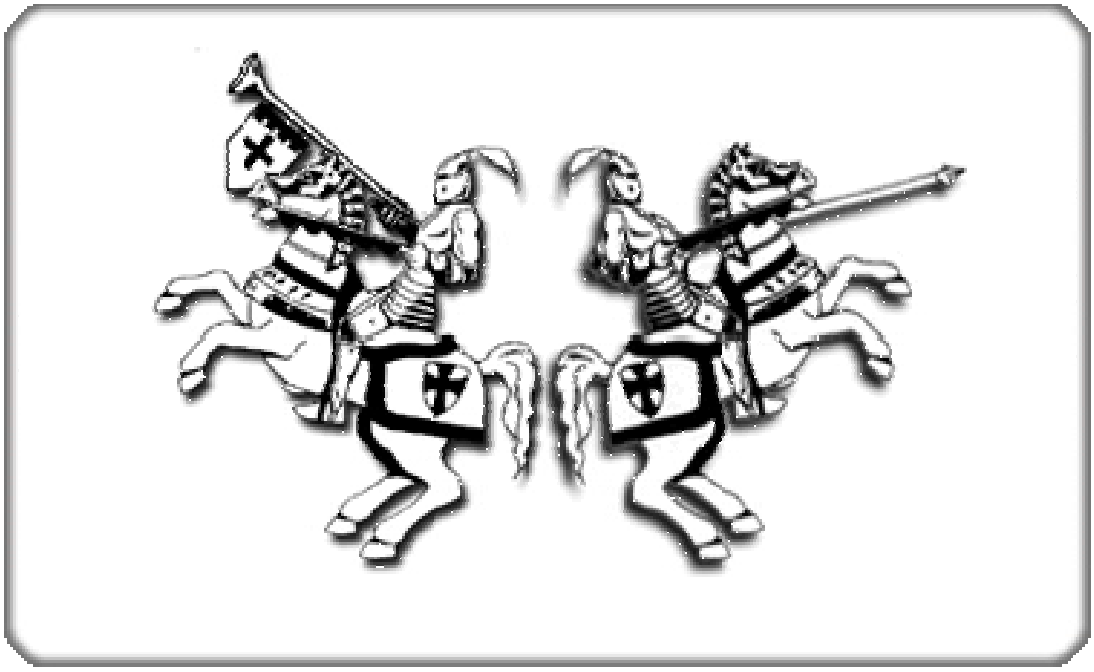
THE KNIGHTS

Risk Assessment



Information Security Risk Assessment For

The Knights Inc.

Version 1.0

March 2014

Prepared For:

The Knights Inc.
112 E. Koch Street

Risk Assessment Annual Document Review History

Review Date	Reviewer
March, 2014	Jane Jones

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

TABLE OF CONTENTS

LIST OF EXHIBITS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

Staff The Knights Inc performed this risk assessment for Information Systems and assets of the company to satisfy the requirements of ISO 27001:2013 to perform an assessment at least every 3 years or whenever a major change is made to a sensitive system. The initial risk assessment for this system was completed on March 10, 2014.

This risk assessment builds upon information and data on the assets collected within the past 12 month. In addition, an IT Security Audit, conducted by The Knights Internal Audit staff on February 24, 2014 was utilized. This risk assessment was performed in accordance with a methodology described below, and utilized interviews and questionnaires developed by The Knights staff to identify the information systems

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

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

- **Camila Jones, The Knights Information Security Officer, reviewed the Risk Assessment report prior to completion;**
- **Rajesh Patel, The Knights Information System Manager, managed the risk assessment process, using The Knights Risk Management staff to conduct the risk assessment, as well as providing information through interviews and completing questionnaires.**
- **Robert Williams, The knight Data Manager, provided information through interviews and through completing questionnaires;**
- **Joshua Michaels, Data manager, provided information through interviews and through completing questionnaires;**
- **Heather Roberts, System Administrator provided required technical information regarding the Knights information systems and asset, through interviews and questionnaires.**

Table A defines the risk levels (high, moderate, low) adopted to classify risks to the Knights, in the defined context of the organization.

Table A: Risk Classifications

Risk Level	Risk Description
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

IT system characterization defines the scope of the risk assessment effort. The team utilised the previously-developed IT System Inventory and Definition Document (Appendix B of the Guideline) as input for this step; some additional information was gathered. 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 Identification

IT System Identification

Table B: IT System Inventory and Definition

IT System Inventory and Definition Document			
I. IT System Identification and Ownership			
IT System ID	THE KNIGHTS INC.-001	**IT System Common Name**	The Knight Information System (KIS)
Owned By	The Knights Inc		
Physical Location	Data Center 112 Koch Street		
Major Business Function	Enable processing of information required to provide the business services		
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)	Robert Williams (804) 979-3452 Joshua Michaels (804) 979-3455	**Data Custodian(s) Phone Number(s)**	Heather Roberts Partner Systems, Inc. (888) 989-8989
Other Relevant Information	The Knights Information system (KIS) has been in production since December 2009		

Table B: System Inventory and Definition (continued)

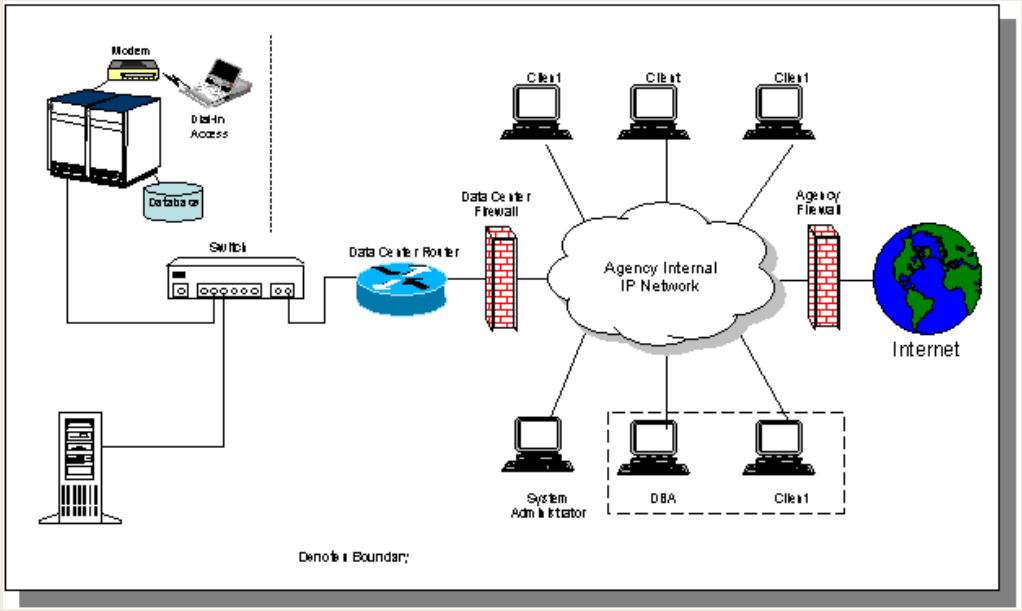
II. IT System Boundary and Components	
IT System Description and Components	KIS is a distributed client-server application transported by a network provided by PSI, a third-party. The major components of the KIS include: • A Sparc SUNW, Ultra Enterprise 3500 server running SunOS 5.7 (Solaris 7). The 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 THE KNIGHTS INC. under contract by PSI, and this Risk Assessment relies on information regarding system hardware and Operating System software provided to the Knights by PSI. • One (1) network interface that is connected to Knight's data center Cisco switch. This interface is assigned two unique IP addresses. • An Oracle 9i data store with two (2) commercial off-the-shelf (COTS) application modules (ABC and XYZ) purchased from Oracle Corporation.
IT System Interfaces	• An interface between the head office and branch office. This interface allows only the KIS to securely transmit data using the Secure Copy Protocol (SCP) on port 22 into the KIS nightly by a cron job that refreshes tables in the KIS Oracle store with selected data from KIS tables. • A modem for emergency dial-in support and diagnostics, secured via the use of a one-time password authentication mechanism. • Client software located within the Knight's Windows 2003 Server Active Directory Domain to manage access to KIS. 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 Knight's Domain can access the client software, although a separate client login and password is required to gain access to KIS data and functions. This access is based on Oracle roles and is granted by the KIS system administrators to users based on their job functions.
IT System Boundary	• The demarcation between the KIS and the Local Area Network (LAN) is the physical port on the Cisco switch that connects the KIS to the network. The switch and other network components are not considered to be part of the KIS. • KIS support personnel provide the operation and maintenance of the application. The KIS personnel provide the operation and maintenance of the server and operating system. The KIS boundary is the following directories and their sub-subdirectories: /var/opt/Oracle, /databases/Oracle, and /opt/odbc. Other directories are outside the KIS boundary. • Client access to the KIS server is controlled by Knights's Windows 2003 Server Active Directory domain. This access are included within the KIS system boundary.

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**
Knights	Busines Information System	BIS (KIS)	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**
Customer company profiles	Low Data is public information	Moderate	Moderate Data is used less than daily by all Knights associates
Customer consultancy reports	High Release of the data could be damaging customers image and competitive advantage	Moderate	High Daily work performed
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

Figure 1: IT System Boundary Diagram



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.

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

The Knights Information System (KIS) is in the implementation phase of its life cycle. Accordingly, identification of vulnerabilities for KIS included:

- **Interviews with the System "Owner", Data "Owner", and operational and technical support personnel;**
- **Use of automated tools; and**
- **Review of vulnerabilities identified in previous 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. The personnel of The Knights Inc. are encouraged to consult other threat information sources. 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.

3.2 Identification of Credible Threats

Credible threats to the KIS were identified by:

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

Table C: Credible Threats Identified for the KIS

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 and;
- 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 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 KIS 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 KIS.

Table D: Vulnerabilities, Threats, and Risks

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

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

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

4 CONTROL ANALYSIS

The purpose of this step is to document a list of security controls used for the IT system based on Annex A of ISO 27001:2013. 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 treatment.

Table E: Security Controls

Control Area	In-Place/ Planned	Description of Controls
1 Risk Management		
IT Security Roles & Responsibilities	In place	1. Required IT Security roles have been assigned in writing, both for THE KNIGHTS INC. as a whole, & for the KIS. John Howard, THE KNIGHTS INC. Commissioner, has designated Jane Jones as THE KNIGHTS INC. ISO & delegated the assignment of other IT security roles to her. 2. With respect to KIS, Jane Jones has assigned individuals to the required IT security roles, as documented elsewhere in this report.
Business Impact Analysis	In place	1. THE KNIGHTS INC. management & staff conducted & documented a Business Impact Analysis (BIA) of the Agency during June 2004; this BIA was updated in May 2007. The THE KNIGHTS INC. BIA notes that the KIS supports essential THE KNIGHTS INC. functions.
IT System & Data Sensitivity Classification	In place	1. THE KNIGHTS INC. has documented classification of the sensitivity of THE KNIGHTS INC. IT systems & data, including the KIS. This classification notes the high sensitivity of much of the data handled by the KIS.
IT System Inventory & Definition	In place	1. THE KNIGHTS INC. has documented an inventory of its sensitive IT systems; this inventory includes the KIS; the System Definition of KIS is included in Section 2 of this Risk Assessment report.
Risk Assessment	In place Planned	1. This report documents the Risk Assessment of KIS in July 2007, building on an earlier KIS Risk Assessment in July 2004. 2. THE KNIGHTS INC. will validate the current Risk Assessment through annual self-assessments in July 2008 & July 2009, & will conduct the next formal KIS RA in July 2010, or sooner, if necessary.
IT Security Audits	In place Planned	1. Anne Keller, THE KNIGHTS INC. Internal Audit Director manages IT Security Audits for THE KNIGHTS INC.. 2. An IT Security Audit of KIS was conducted & documented by THE KNIGHTS INC. Internal Audit staff on June 24, 2007. 3. Required reporting for the KIS CAP is in place. 4. Future IT Security Audits of THE KNIGHTS INC. are planned biennially.
2 IT Contingency Planning		
Continuity of Operations Planning	In place	1. Sam Robinson is the THE KNIGHTS INC. Continuity of Operations Plan (COOP) Coordinator & also serves as the focal point for IT COOP & Disaster Recovery (DR) activities. 2. The THE KNIGHTS INC. COOP documents the requirements for 24-hour recovery of the KIS & its data to support budget preparation, & 72-hour recovery of KIS & its data at other times. 3. The THE KNIGHTS INC. COOP identifies all personnel required for its execution, including personnel required for recovery of the KIS, & includes emergency declaration, notification, & operations procedures. 4. The COOP document is classified as sensitive; access to this document is restricted to COOP team members, & a copy of the COOP is stored off site at Data Recovery Services, Inc., THE KNIGHTS INC.'s recovery site partner. 5. Recovery procedures for KIS were most recently tested during THE KNIGHTS INC.'s annual COOP exercise on May 18-20, 2007.

Table E: Security Controls (continued)

Control Area	In-Place/ Planned	Description of Controls
2 IT Contingency Planning (continued)		
IT Disaster Recovery Planning	In place	1. A Disaster Recovery Plan (DRP) for the KIS has been documented & approved by the THE KNIGHTS INC. Commissioner. This plan calls for recovery of the KIS 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 KIS during budget preparation, the contract with DRSI includes 24-hour recovery during this period. 2. Both 72- & 24-hour recovery of the KIS were tested during the THE KNIGHTS INC. COOP exercise on May 18-20, 2007, including access to the recovered KIS by users at other COV Agencies. Members of the KIS Disaster Recovery Team received training on their responsibilities in advance of the exercise.
	Planned	1. The KIS DRP is currently being updated as a result of the recovery during the THE KNIGHTS INC. COOP exercise; completion is expected by September 1, 2007. 2. Recovery of the KIS will next be tested during the THE KNIGHTS INC. COOP exercise scheduled for May 2008.
IT System & Data Backup & Restoration	In place	1. A Backup & Restoration Plan for the KIS has been documented, & approved by John James, the KIS System Owner. This plan calls for: a. Weekly full & daily incremental backups & review of backup logs of KIS data by operations staff; b. Weekly pickup & transport of KIS backup tapes to DRSI by DRSI personnel; & c. Restoration of KIS data either at THE KNIGHTS INC. or at DRSI only with the express written approval of John James, the KIS System Owner or his designee.
3 IT Systems Security		
IT System Hardening	In place	1. KIS operations staff has identified & documented the Solaris 7 & Oracle 9i benchmarks from the Center for Internet Security (CIS) as appropriate hardening levels for the KIS. John James, the KIS System Owner, has approved this recommendation in writing. These benchmarks were most recently applied to KIS in May 2007, & the application was documented in the KIS Change Log. 2. KIS operations staff most recently reviewed these benchmarks on June 7, 2007, & determined that they continue to provide an appropriate hardening level for the KIS. Benchmarks are reapplied whenever the operating system or application software is changed.
	Planned	3. PSI, the THE KNIGHTS INC. business partner that operates the THE KNIGHTS INC. technology environment, has engaged Cyberscan, Inc. to conduct a full vulnerability scan of the THE KNIGHTS INC. technology environment. This scan is scheduled for August 2007. 4. Based on the results of the vulnerability scan, KIS operations staff will determine whether the CIS benchmarks continue to provide appropriate protection for the KIS.

Table E: Security Controls (continued)

Control Area	In-Place/ Planned	Description of Controls
3 IT Systems Security (continued)		
IT Systems Interoperability Security	In place	1. The KIS receives data only from the BCS; it does not transmit data to any other IT system. This data sharing is documented in Section 2.2 of this Risk Assessment, & in the BCS Risk Assessment. John James is System Owner of both BCS & KIS; therefore no written data sharing agreement is required. Security of network access is covered by a documented interoperability security agreement between John James, KIS System Owner, & Bea Roberts, System Owner of the PSI third-party network.
Malicious Code Protection	In place	1. THE KNIGHTS INC. has two different anti-virus software products installed on its desktop & laptop computers & on its e-mail servers. This software: a. Eliminates or quarantines all malicious programs that it detects & provides an alert to the user upon detection; b. Runs automatically on power-on & runs weekly full scans on memory & storage devices; c. Automatically scans all files retrieved from all sources; d. Allows only system administrators to modify its configuration; & e. Maintains a log of protection activities; f. Eliminates or quarantines malicious programs in e-mail messages & file attachments as they attempt to enter the Agency's e-mail system. 2. Both desktop/laptop & e-mail anti-virus software are configured for automatic download of definition files whenever new files become available.
	Planned	3. The THE KNIGHTS INC. Acceptable Use Policy, under development, will prohibit THE KNIGHTS INC. users from intentionally developing or experimenting with malicious programs & knowingly propagating malicious programs including opening attachments from unknown sources. This policy is scheduled for completion in August 2007.
IT Systems Development Life Cycle Security	In place	1. The KIS is in the Implementation phase of its life cycle. As documented throughout this Risk Assessment report, THE KNIGHTS INC. conducts & documents a formal Risk Assessment of the KIS every three years. In addition the KIS complies with all other Risk Management requirements of the COV IT Security Standard.

Table E: Security Controls (continued)

Control Area	In-Place/ Planned	Description of Controls
4 Logical Access Control		
Account Management	**In place**	**Documented THE KNIGHTS INC. & KIS policies require:** **1. Granting access to IT system users based on the principle of least privilege. In the case of KIS, however, enforcement of least privilege is accomplished by granting ad-hoc access rights to KIS, rather than granting access based on predefined roles.** **2. Approval by John James, KIS System Owner & a prospective KIS user's supervisor before granting access to KIS; these policies are enforced.** **3. Prospective KIS users to receive a THE KNIGHTS INC.-required criminal background check before receiving access to KIS; these policies are enforced.** **4. The use of passwords on all KIS accounts, & that these passwords expire every 90 days, at a minimum. These policies are not enforced on KIS, however, as passwords are not set to expire & password changes are not enforced.** **5. Annual review of all KIS accounts to assess the continued need for the accounts & 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 THE KNIGHTS INC. records retention policy, & notification of supervisors, Human Resources, & the System Administrator about changes in the need for KIS accounts. These policies are not enforced on KIS, however, & KIS user accounts are not removed when the access is no longer required.** **6. Prohibit the use of group accounts & shared passwords. These policies are not enforced on KIS, however, as accounts such as "guest," "test," & "share" exist in the KIS user database.** **7. John James to approve access changes to KIS accounts, & for John James & the KIS operations & support team to investigate unusual account access. These policies are enforced.**
Password Management	**In place**	**Documented THE KNIGHTS INC. & KIS policies require:** **1. The use of passwords on sensitive systems such as KIS; these policies are enforced on KIS. These policies also require that, at a minimum, passwords be no less than eight characters long & contain both letters & numbers; Windows Active Directory is configured to require this length & complexity for KIS passwords.** **2. Encryption of passwords during transmission; password encryption, however, is not correctly configured for KIS & KIS passwords are transmitted in clear text.** **3. Users to maintain exclusive control of their passwords, to allow users to change their passwords at will, & to change a password immediately & notify the ISO if the password is compromised; these policies are enforced.** **4. KIS users to change passwords every 90 days at a minimum; as noted above, however, these policies are not enforced with respect to KIS.** **5. The use of password history files to present password re-use; these policies are enforced on KIS & KIS retains the previous 240 passwords for each user to prevent their re-use.**

Table E: Security Controls (continued)

Control Area	In-Place/ Planned	Description of Controls
4 Logical Access Control (continued)		
Password Management (continued)	In place	Documented THE KNIGHTS INC. & KIS policies require: 7. Use of a procedure for delivery of the initial KIS password in person from the KIS support team in a sealed envelope. The password is expired, & the user is forced to change the password upon first login. Forgotten initial passwords are replaced by the KIS support team & not re-issued. 8. Prohibit the use of group accounts & shared passwords. These policies are not enforced on KIS, however, as accounts such as "guest," "test," & "share" exist in the KIS user database. 9. Prohibit the inclusion of passwords as plain text in scripts. These policies are not enforced on KIS, however, as passwords are included in scripts & initialization files. 10. Limit access to files containing KIS passwords to the KIS support team. These policies are enforced. 11. Suppression of passwords on the screen as they are entered. These policies are enforced. 12. Members of the KIS support team to have both an administrative & user account & use the administrative account only when performing tasks that require administrative privileges. These policies are enforced. 13. At least two members of the KIS support team to have KIS administrative account.
Remote Access	In place	1. Based on the sensitivity of KIS data, documented THE KNIGHTS INC. & KIS policies require that remote access to KIS not be permitted from outside the PSI-provided third-party network. Remote OS authentication, however, is enabled in the KIS application, even though no user accounts are configured to allow this access.
	Planned	2. To enable alternate work schedules, & work locations, THE KNIGHTS INC. is in the process of developing a plan to allow secure remote access to KIS. This plan is scheduled for completion in October 2007.
5 Data Protection		
Data Storage Media Protection	In place	Documented THE KNIGHTS INC. & KIS policies require: 1. Bea Roberts, as KIS Data Custodian, to provide protection of all sensitive KIS data. These requirements are enforced a written agreement between THE KNIGHTS INC. &Partner Services, Inc. 2. Sensitive KIS data not to be stored on mobile data storage media through THE KNIGHTS INC. policy that prohibits local storage of KIS data. This policy is not enforced, however, as sensitive KIS data is stored on USB drives. 3. Only authorized DRSI personnel to pickup, receive, transfer, & deliver KIS tapes. This policy is enforced. 4. KIS administrators & users to follow the ITRM Removal of Commonwealth Data from Surplus Computer Hard Drives & Electronic Media Standard (ITRM Standard SEC2003-02.1) when disposing of KIS data storage media that are no longer needed. This policy is enforced. 5. KIS users to receive training on the proper procedure for disposal of data storage media containing sensitive data as part

Table E: Security Controls (continued)

5 Data Protection (continued)		
Encryption	**In place**	**KIS uses encryption via:** **1. The secure shell (ssh) & secure copy (scp) protocols, which are in wide commercial use. This use is documented in KIS design documents.** **2. The CRDSK hard disk encryption product, as documented in THE KNIGHTS INC. & KIS policies.** **3. Encryption of passwords during transmission. As noted above, however, this feature is incorrectly configured for KIS; KIS passwords are transmitted in clear text.**
	Planned	**4. THE KNIGHTS INC. is currently documenting Agency policies, standards, & procedures for encryption technologies. Completion of this documentation is planned by October 1, 2007.**
6 Facilities Security		
Facilities Security	**In place**	**1. The KIS is housed in the THE KNIGHTS INC. Data Center with access controlled via a Secure card-key access system, administered by the THE KNIGHTS INC. IRM staff, which permits monitoring, logging, & auditing of all access to the THE KNIGHTS INC. Data Center. Jane Jones, THE KNIGHTS INC. ISO approves all requests for THE KNIGHTS INC. Data Center Access requests based on the principle of least privilege.** **2. The THE KNIGHTS INC. Data Center is heated & cooled by a 90-ton HVAC unit, separate from the HVAC unit that heats & cools the remainder of the facility. Electric power to the THE KNIGHTS INC. 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.** **3. Fire suppression in the THE KNIGHTS INC. Data Center is provided by a wet-pipe sprinkler system. THE KNIGHTS INC. is aware that this fire suppression system poses a risk of significant water damage to equipment in the data center, including KIS. Replacement of the wet-pipe sprinkler system, however, has been considered & is cost-prohibitive.** **4. Access to the THE KNIGHTS INC. facility at 123 Elm St. is also protected by the Secure card-key access system, administered by the THE KNIGHTS INC. IRM staff. Cards that permit access to the facility are given only to THE KNIGHTS INC. employees & contractors upon supervisory approval. All visitors are required to have escorts in the THE KNIGHTS INC. facility.** **5. Access to other areas in the THE KNIGHTS INC. facility that house IT resources is controlled via means of cipher locks, also administered by the THE KNIGHTS INC. IRM staff, which changes the lock ciphers every 90 days. Jane Jones, THE KNIGHTS INC. ISO approves all requests for access to the lock cipher based on the rule of least privilege.**

Table E: Security Controls (continued)

7 Personnel Security		
Access Determination & Control	**In place**	**1. KIS users receive a THE KNIGHTS INC.-required fingerprint criminal background check & a credit check before receiving access to KIS.** **2. Access to the THE KNIGHTS INC. facility & the THE KNIGHTS INC. Data Center that houses the KIS is controlled by card-key access.** **3. Adequate separation of duties exists for KIS in order to guard against the possibility of fraud.** **Documented THE KNIGHTS INC. & KIS policies require:** **4. The removal of physical & 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 KIS.** **5. Return of Agency assets upon transfer or termination. These policies are enforced.** **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 KIS, however, enforcement of least privilege is accomplished by granting ad-hoc access rights to KIS, rather than granting access based on predefined roles.**
IT Security Awareness & Training	**In place**	**1. Jane Jones, THE KNIGHTS INC. ISO, is responsible for THE KNIGHTS INC.'s IT security awareness & training program. THE KNIGHTS INC. requires, through documented policies & procedures, that all employees & 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 THE KNIGHTS INC.'s specifications, both records completion & forwards records of completion to the THE KNIGHTS INC. ISO. The online training program covers:** **a. THE KNIGHTS INC. policies for protecting IT systems & data, with a particular emphasis on sensitive systems & data;** **b. The concept of separation of duties;** **c. Employee responsibilities in continuity of operations, configuration management, & incident detection & reporting;** **d. IT system user responsibilities & best practices in:** **1. Prevention, detection, & eradication of malicious code;** **2. Proper disposal of data storage media; &** **3. Proper use of encryption products;** **e. Access controls, including creating & changing passwords & the need to keep them confidential;** **f. THE KNIGHTS INC. Remote Access policies; &** **g. Intellectual property rights, including software licensing & copyright issues.** **2. THE KNIGHTS INC. employees & contractors are required to accept THE KNIGHTS INC. IT security policies by completing an online agreement during the online IT security training.** **3. Members of the KIS support team, THE KNIGHTS INC. DR & Incident Response (IR) team members, & 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 THE KNIGHTS INC. policy, which is enforced.** **4. THE KNIGHTS INC. policy requires that all employees & contractors complete required basic IT security training within**

Table E: Security Controls (continued)

7 Personnel Security (continued)		
Acceptable Use	**In place** **Planned**	**1. THE KNIGHTS INC. 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. THE KNIGHTS INC. employees & contractors are required to agree to this policy by completing an online agreement at the conclusion of online IT security training.** **2. THE KNIGHTS INC. is in the process of developing its own Acceptable Use policy. Completion is expected in December 2007.**
8 Threat Management		
Threat Detection	**In place**	**Jane Jones, THE KNIGHTS INC. ISO is responsible for THE KNIGHTS INC.'s threat detection program, which includes the following components:** **1. THE KNIGHTS INC. IRM staff receive threat detection training annually as their advanced IT security training.** **2. PSI has deployed & monitors Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS) are in the THE KNIGHTS INC. environment.** **3. PSI security staff maintains regular communication with US-CERT & other security research & coordination organizations, review IDS & IPS logs in real-time, & recommend appropriate measures to THE KNIGHTS INC..**
Incident Handling	**In place**	**THE KNIGHTS INC. has documented & enforces:** **1. An Incident Response Team that includes the THE KNIGHTS INC. ISO, THE KNIGHTS INC. ISRM staff, & PSI support & security staff.** **2. A protocol to use IT Security Audits, Risk Assessments, & post-incident review to identify appropriate measures to defend against & respond to cyber attacks.** **3. Proactive measures to prevent cyber attacks in response to recommendations from the PSI security staff.** **4. Internal THE KNIGHTS INC. incident investigation, reporting, & recording processes.** **PSI has documented & enforces on THE KNIGHTS INC.'s behalf:** **5. Proactive measures to prevent cyber attacks in response to recommendations from the PSI security staff.** **6. Incident categorization & prioritization criteria, along with procedures to respond to each level of attack.** **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.**
Security Monitoring & Logging	**In place**	**THE KNIGHTS INC. has documented designation of PSI security staff as responsible for:** **1. Development of logging capabilities & review procedures for THE KNIGHTS INC. as a whole, as well as for the KIS.** **2. Enabling logging on all KIS components & retention of logs for 90 days.** **3. Monitoring KIS security logs in real time & alerts the KIS**

Table E: Security Controls (continued)

9 IT Asset Management		
IT Asset Control	**In place**	**Documented & enforced THE KNIGHTS INC. & KIS policies require:** **1. No THE KNIGHTS INC. IT assets to be removed from THE KNIGHTS INC. premises, except for laptop computers assigned to individual THE KNIGHTS INC. employees.** **2. No IT assets not owned by THE KNIGHTS INC. to be connected to any THE KNIGHTS INC. system or network.** **3. Removal of data from THE KNIGHTS INC. IT assets prior to disposal in accordance with the COV Removal of Commonwealth Data from Surplus Computer Hard Drives & Electronic Media Standard (ITRM Standard SEC2003-02.1).**
Software License Management	**In place**	**1. Documented THE KNIGHTS INC. policies require the use of only THE KNIGHTS INC.-approved software on its IT systems & require annual reviews of whether all software is used in accordance with license requirements.** **2. All KIS software is appropriately licensed.**
Configuration Management & Change Control	**In place**	**1. THE KNIGHTS INC. has document configuration management & change control policies adequate so that changes to the IT environment do not introduce additional IT security risk. THE KNIGHTS INC. enforces these policies with respect to the KIS.**

Identify the security controls for each risk identified in Table D above. Associate the risks with the relevant controls in Annex A of ISO 27001:2013, as below. This correlation determines whether controls exist that respond adequately to the identified risks. Additional controls might have to be devised to cover all 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 KIS identified in Table D with relevant KIS IT security controls documented in Table E and with other mitigating or exacerbating factors.

Table F: Risks-Controls-Factors Correlation

Risk No.	Risk Summary	Correlation of Relevant Controls & Other Factors
1	Fire would activate sprinkler system causing water damage & compro-mising the availability of KIS.	There are no controls relevant to this risk; neither are there any mitigating or exacerbating factors. THE KNIGHTS INC. Executive Management has accepted this risk.
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of KIS 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 of confidentiality & integrity of KIS 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 KIS 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 KIS 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 THE KNIGHTS INC. 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 [illegible]

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 KIS 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 KIS. 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 KIS data.	Controls 4.1.4 and 4.2.4 require regular password changes, but are not enforced for KIS. Support for required password changes is built into the software but have not been enabled.
8	Use of generic KIS accounts could result in compromise of confidentiality & integrity of sensitive KIS data.	Controls 4.1.6 and 4.2.8 require that shared accounts such as these not be used but have not enforced for KIS.
9	Remote access is not currently used by KIS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive KIS data.	Control 4.3.1 prohibits access to KIS 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 KIS.
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive KIS data.	Controls 4.2.9 and 4.5.3 require encryption of passwords, but have not been enforced for KIS. 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 KIS data.	Control 4.4.2 prohibits storage of sensitive KIS data on portable media such as USB drives, but has not been enforced for KIS.

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

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 KIS.

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 KIS and assigns a likelihood, as defined in Table G, to each KIS risk documented in Table D.

Table H: Risk Likelihood Ratings

Risk No.	Risk Summary	Risk Likelihood Evaluation	Risk Likelihood Rating
1	Fire would activate sprinkler system causing water damage & compromising the availability of KIS.	There are no controls against water damage to KIS 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 THE KNIGHTS INC. Data Center is low.	Moderate
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of KIS data.	Effectiveness of controls for closing user accounts is low, as unneeded user IDs exist on KIS. 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 KIS 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 KIS 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 KIS in this manner is limited.	Moderate
5	Exploitation of unpatched application security flaws could compromise confidentiality & integrity of KIS data.	Effectiveness of controls to require timely application of patches to KIS 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

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 confi-dentiality & integrity of KIS 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 KIS 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 KIS accounts could result in compromise of confidentiality & integrity of sensitive KIS 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 KIS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive KIS 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 KIS.	High
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive KIS 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 KIS 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

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.

6 Risk Impact Analysis

Table I documents the ratings used to evaluate the impact of KIS risks on the COV and THE KNIGHTS INC..

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.

Table I: Risk Impact Rating Definitions

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

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 KIS, including the estimated impact for each risk identified in Table D and the impact rating assigned to the risk.

Table J: Risk Impact Analysis

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

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 KIS. 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. THE KNIGHTS INC.'s most recent Business Impact Analysis (BIA) was reviewed in determining the ratings.

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 KIS.

Table K: Overall Risk Rating Matrix

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

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

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 KIS.

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 availabil-ity of KIS.	Moderate	High	Moderate
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of KIS data.	Moderate	High	Moderate
3	Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of KIS data.	Moderate	High	Moderate
4	Denial of service attack via large bogus packets sent to port 1521 could render KIS unavailable for use.	Moderate	High	Moderate
5	Exploitation of un-patched application security flaws could compromise confidentiality & integrity of KIS data.	Moderate	High	Moderate
6	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of KIS data.	Moderate	High	Moderate

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 KIS data.	Moderate	High	Moderate
8	Use of generic KIS accounts could result in compromise of confidentiality & integrity of sensitive KIS data.	High	High	High
9	Remote access is not currently used by KIS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive KIS data.	High	High	High
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive KIS data.	Moderate	High	Moderate
11	Loss or theft of USB drives could result in compromise of confidentiality of KIS 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."

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 KIS system.

Table M: Recommendations

Risk No.	Risk Summary	Risk Rating	Recommendations
1	Fire would activate sprinkler system causing water damage & compromising the availability of KIS.	Moderate	None. Replacing the wet-pipe sprinkler system in the THE KNIGHTS INC. Data Center has been determined to be cost-prohibitive. THE KNIGHTS INC. executive management has elected to accept this risk.
2	Unauthorized use of unneeded user IDs could compromise confidentiality & integrity of KIS data.	Moderate	The KIS support team should follow THE KNIGHTS INC. & KIS policies regarding removal of accounts. THE KNIGHTS INC. IRM should develop & implement a process to verify that termination procedures are carried out in the timeframe specified by THE KNIGHTS INC. & KIS policy.
3	Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of KIS data.	Moderate	THE KNIGHTS INC. IRM should develop KIS user roles & associated privileges. Once developed the KIS support team should implement these roles & assign KIS privileges based on role.
4	Denial of service attack via large bogus packets sent to port 1521 could render KIS	High	THE KNIGHTS INC. 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

Table M: Recommendations (continued)

Risk No.	Risk Summary	Risk Rating	Recommendations
5	Exploitation of unpatched application security flaws could compromise confidentiality & integrity of KIS data.	Moderate	The KIS 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 con-fidentiality & integrity of KIS 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 KIS data.	Moderate	The KIS support team should enable the functionality within Oracle to expire passwords & require changes.
8	Use of generic KIS accounts could result in compromise of confidentiality & integrity of sensitive KIS data.	High	The KIS support team should remove all generic accounts from KIS. THE KNIGHTS INC. IRM should monitor accounts should continue to verify that no new shared accounts are created.
9	Remote access is not currently used by KIS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive KIS data.	High	As an immediate step, the KIS support team should disable the remote OS feature. As documented in planned controls, the THE KNIGHTS INC. IRM staff and KIS support team should work to develop a secure method to allow remote access to KIS.
10	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive KIS data.	Moderate	The KIS support team should configure the login encryption feature properly.
11	Loss or theft of USB drives could result in compromise of confidentiality of KIS data.	High	THE KNIGHTS INC. should include the prohibition on storing sensitive data on removable media such as USB drives in the THE KNIGHTS INC. Acceptable Use policy, under development, and in the THE KNIGHTS INC. Security Awareness and Training program.

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 KIS Data Center.	Fire	Compromise of KIS availability.	Fire would activate sprinkler system causing water damage & compro-mising the availability of KIS.	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 THE KNIGHTS INC. Data Center has been determined to be cost-prohibitive. THE KNIGHTS INC. executive management has elected to accept this risk.
2	KIS user identifiers (IDs) no longer required are not removed from KIS in timely manner.	Unauth-orized Use	Compromise of confiden-tiality & integrity of KIS data.	Unauthorized use of unneeded user IDs could compromise confidential-ity & integrity of KIS 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 KIS support team should follow THE KNIGHTS INC. & KIS policies regarding removal of accounts. THE KNIGHTS INC. IRM should develop & implement a process to verify that termination procedures are carried out in the timeframe specified by THE KNIGHTS INC. & KIS policy.
3	KIS access privileges are granted on an ad-hoc basis rather than predefined roles.	Unauthor-ized Access	Compromise of confiden-tiality & integrity of KIS data.	Unauthorized access via ad-hoc privileges could compromise of confidentiality & integrity of KIS 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.	THE KNIGHTS INC. IRM should develop KIS user roles & associated privileges. Once developed the KIS support team *should* implement these roles & assign KIS 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 KIS to stop responding.	Malici-ous Use Com-puter Crime	Compromise of KIS availability.	Denial of service attack via large bogus packets sent to port 1521 could render KIS 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.	THE KNIGHTS INC. 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.	Malici-ous Use Comp-uter Crime	Compromise of confiden-tiality & integrity of KIS data.	Exploitation of un-patched application security flaws could compromise confidentiality & integrity of KIS 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 KIS 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 KIS data.	Exploitation of passwords in script & initialization files could result in compromise of confidentiality & integrity of KIS 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 KIS. 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 KIS data.	Compromise of unexpired/ unchanged passwords could result in compromise of confidentiality & integrity of KIS data.	Moderate	High	Moderate	Controls 4.1.4 and 4.2.4 require regular password changes, but are not enforced for KIS. Support for required password changes is built into the software but have not been enabled.	The KIS 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 KIS data.	Use of generic KIS accounts could result in compromise of confidentiality & integrity of sensitive KIS 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 KIS.	The KIS support team should remove all generic accounts from KIS. THE KNIGHTS INC. IRM should monitor accounts should continue to verify that no new

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 KIS data.	Remote access is not currently used by KIS; enabling this access when not necessary could result in compromise of confidentiality & integrity of sensitive KIS data.	High	High	High	Control 4.3.1 prohibits access to KIS 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 KIS.	As an immediate step, the KIS support team should disable the remote OS feature. As documented in planned controls, the THE KNIGHTS INC. IRM staff and KIS support team should work to develop a secure method to allow remote access to KIS.
10	Login encryption setting is not properly configured.	Malicious Use Computer Crime	Compromise of confidentiality & integrity of KIS data.	Unencrypted passwords could be compromised, resulting in compromise of confidentiality & integrity of sensitive KIS data.	Moderate	High	Moderate	Controls 4.2.9 and 4.5.3 require encryption of passwords, but have not been enforced for KIS. Physical security protections are in place that would limit the ability to sniff the network to exploit this vulnerability.	The KIS support team should configure the login encryption feature properly.
11	Sensitive KIS data is stored on USB drives	Malicious Use Computer Crime	Compromise of confidentiality of KIS data.	Loss or theft of USB drives could result in compromise of confidentiality of KIS data.	High	High	High	Control 4.4.2 prohibits storage of sensitive KIS data on portable media such as USB drives, but has not been enforced for KIS.	THE KNIGHTS INC. should include the prohibition on storing sensitive data on removable media such as USB drives in the THE KNIGHTS INC. Acceptable Use policy, under development, and in the THE KNIGHTS INC. Security Awareness and Training program

RISK ASSESSMENT REPORT TEMPLATE

Information Technology Risk Assessment For

Risk Assessment Annual Document Review History

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

Review Date	Reviewer

TABLE OF CONTENTS

LIST OF EXHIBITS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Risk assessment participants:

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

Risk assessment techniques used:

Table A: Risk Classifications

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

2 IT SYSTEM CHARACTERIZATION

Table B: IT System Inventory and Definition

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

Rating and Classification	IT System Classification Must be “Sensitive” if overall sensitivity is “high”; consider as “Sensitive” if overall sensitivity is “moderate”	
	SENSITIVE	**NON-SENSITIVE**

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

Figure 1 – IT System Boundary Diagram

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

Figure 2 – Information Flow Diagram

3 RISK IDENTIFICATION

Identification of Vulnerabilities

Vulnerabilities were identified by:

Identification of Threats

Threats were identified by:

The threats identified are listed in Table C.

Table C: Threats Identified

Identification of Risks

Risks were identified by:

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

Table D: Vulnerabilities, Threats, and Risks

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

4 CONTROL ANALYSIS

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

Table E: Security Controls

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

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

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

Table F: Risks-Controls-Factors Correlation

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

5 RISK LIKELIHOOD DETERMINATION

Table G defines the risk likelihood ratings.

Table G: Risk Likelihood Definitions

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

Table G, evaluates the effectiveness of controls and the probability or motivation and capability of each threat to KIS 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 No.	Risk Summary	Risk Likelihood Evaluation	Risk Likelihood Rating
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.

Table I: Risk Impact Rating Definitions

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

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

Table J: Risk Impact Analysis

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

Risk No.	Risk Summary	Risk Impact	Risk Impact Rating
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 x 1.0 = 10	Moderate 50 x 1.0 = 50	High 100 x 1.0 = 100
Moderate (0.5)	Low 10 x 0.5 = 5	Moderate 50 x 0.5 = 25	Moderate 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

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

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

Table L: Overall Risk Ratings Table

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

Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
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.

Table M: Recommendations

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

9 RESULTS DOCUMENTATION

Exhibit 1: Risk Assessment Matrix

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