Now that you have finished the class, it is time to wrap up. You have been working at your company for a year now and the CEO is asking you to put together a Risk Assessment for the organization. You may use ONE of the two structural aides below:

* this template <https://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Word_versions/Risk_Assessment_Instructions.doc>

  OR

* the structure in chapter 3 of this document <http://ithandbook.ffiec.gov/media/27466/nis-risk_mang_guide_infor_tech_systems_pub_800_30.pdf>

to create a simplified RA for the year based on all the in-class work and the labs you have completed so far. You may customize it to fit your company. You may also review a few online examples like [this one](http://www.cio.ca.gov/OIS/Government/documents/docs/RA_SampleReport.doc).

IN A MS WORD DOCUMENT (10 points each):

1. Provide an organizational IT Risk Assessment using the given template.

**NIST800-27002**

**ISO 9001:2000**

**Guidelines SEC562-05**

**Version IV – Risk Assessment Instructions**

**Effective Date: 05/06/2017**

**Green Disk Videos and Video Games**



**Information Technology Resource Management**

**Information Technology Risk Assessment Guideline**

**Version IV – Risk Assessment Instructions**

Green Disk Video and Video Games (GDVVG)

**Organization Overview**

GreenDisk Videos and Video Games is a provider of “wholesome entertainment,” delivering highly edited (for violence, language, nudity, and moral issues) mainstream movies, religious films, and games with morally wholesome content to its users through a computer, an Android and an iPhone app, or a Roku channel, for $7.99 a month. Its headquarters are in Burbank, CA, with all customer-facing IT operations based in Palo Alto, CA.

GreenDisk’s 1,500 employees serve upwards of 2,000,000 subscribers; the company has budgets in excess of $100 million dollars and complies with various regulations. To meet the needs of all these constituencies, GreenDisk has all the business processes and IT systems found in a typical service corporation such as HR, payroll, finance, marketing and customer relations, and billing, in addition to typical services such as email and calendar. Quite naturally, GreenDisk has a large IT department, which is dedicated to ensuring that sensitive customer data, such as credit card numbers, birthdates, and other information, is kept absolutely secure while providing a highly customized user experience.

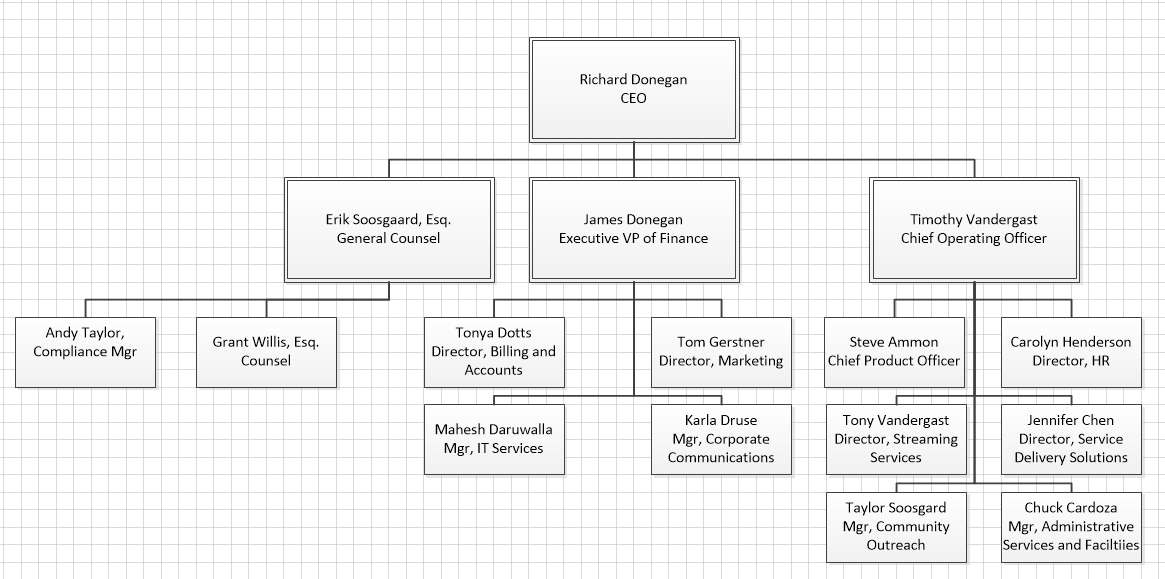
Hoping to capitalize on the current political situation, GreenDisk is pursuing a joint venture with a Hollywood megachurch to produce “L.A. Miracle,” a TV show about miracles in the lives of Los Angeles, CA, citizens. The recently hired producer and his staff of writers have a strong record of attracting donations from viewers, but while this project creates great opportunities for local actors to achieve more visibility, the IT department has been advised that it should upgrade its systems for handling pre-production, production, and post-production assets. Two years ago, one of the main streaming servers was hacked with a redirect to an adult video provider, and sensitive customer information was stolen for all new customer accounts set up right before the redirect was planted.

In addition to its regular and new business activities, GreenDisk also supports two major community outreach efforts:

1. An annual Young Filmmaker’s Talent Competition, in which high school and college students are invited to use the company’s IT resources and mentoring from executives to produce a short film, with which they compete for a $10,000 scholarship to a local filmmaker school.
2. An annual donation drive for, and job fair at, a local homeless shelter, complete with providing resume services and mock interviews.

**Organization Structure**

An extract from the company’s organizational structure is shown below. Your work in this course will be limited to these units of the business. The Chief Executive Officer is responsible for the overarching business strategy and goals. The Executive Vice President of Finance is responsible for all marketing and finance activities. General Counsel manages legal affairs and compliance, and the Chief Operating Officer is responsible for all activities in support of the company’s business.



The company’s business and finance services are largely centralized. The administrative services component handles purchasing, physical building maintenance, and safety. HR deals with payroll, hiring procedures, and benefits. IT Services owns the Enterprise Business Systems, including HR systems, and payroll and financial systems, but Service Delivery Solutions owns all customer-focused hardware and software.

Some ancillary IT services are operated as a mix of centralized services and local support. These services include desktop support and management, file share management, print management, account provisioning, and server management. To save costs, the management of some of these services is led by administrative assistants whose primary responsibility is to support departmental administrative needs. Generally speaking, technical staff is over-worked, under paid, but is well-trained and qualified. They do their best to meet stakeholder expectations on a limited budget. The information security department split between IT Services and Service Delivery Solutions.

Table of contents

[PURPOSE, Cautions & FORMAT 1](#_Toc153702090)

[Example Risk Assessment 2](#_Toc153702091)

[RISK ASSESSMENT REPORT Template 49](#_Toc153702095)

Information Technology Risk Assessment For

Budget Formulation Agency

Budget Formulation System

Version 4.0

May 2017

Prepared For:

Green Disk Video and Video Games

Development Team of Green Disk Video

Burbank, CA,

Prepared By:

Green Disk Risk Analysis Department

Risk Assessment Division

1433 Christopher Center,

Valparaiso, IN 46383

***Risk Assessment Annual Document Review History***

|  |  |
| --- | --- |
| **Review Date** | **Reviewer** |
| **Jan, 2017** | **Sonja Streuber** |
| **May, 2017** | **Sonja Streuber** |
|  |  |

The conditions of the risk assessment change as the Development 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**

[**1 INTRODUCTION 7**](#_Toc142921514)

[**2 IT SYSTEM CHARACTERIZATION 9**](#_Toc142921515)

[**3 RISK IDENTIFICATION 14**](#_Toc142921516)

[**4 CONTROL ANALYSIS**](#_Toc142921517) **20**

1 INTRODUCTION

Green Disk Videos and Video Games is a provider of “wholesome entertainment,” delivering highly edited (for violence, language, nudity, and moral issues) mainstream movies, religious films, and games with morally wholesome content to its users through a computer, an Android and an iPhone app, or a Roku channel, for $7.99 a month. Its headquarters are in Burbank, CA, with all customer-facing IT operations based in Palo Alto, CA.

In addition to its regular and new business activities, Green Disk also supports two major community outreach efforts:

1. An annual Young Filmmaker’s Talent Competition, in which high school and college students are invited to use the company’s IT resources and mentoring from executives to produce a short film, with which they compete for a $10,000 scholarship to a local filmmaker school.
2. An annual donation drive for, and job fair at, a local homeless shelter, complete with providing resume services and mock interviews.

Risk Assessment and analysis team are encouraged to classify risks as High, Moderate or Low in accordance with the definitions in the Standard. The definitions of risk classifications should be included in Table A of the Risk Assessment Report.

**1 Introduction**

**Staff of the Green Disk Video and Video Games Budget Formulation Agency (BFA) performed this risk assessment for the Budget Formulation System (BFS) to satisfy the requirement of ISO Stand of ISO 9001-2000 to perform an assessment at least every 2 years or whenever a major change is made to a sensitive system. The last risk assessment for this system was completed on May 6, 2017.**

**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 May 6, 2017 was utilized. This risk assessment was performed in accordance with a methodology described in ISO Guidelines ISO 9001-2001, and utilized interviews and questionnaires developed by BFA staff to identify BFS**

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

1. Table A defines the risk levels (high, moderate, low) adopted to classify risks to the Agency, in the context of the BIA.
2. Table 2: Risk Levels

1. 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. 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.

2.2 IT System Boundary & Components included in the Risk Assessment

1. 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** | **Development Team of Green Disk (BFA)**  **Financial Operations Division (FOD)** | | | | |
| **Physical Location** | **Data Center**  Burbank, CA, | | | | |
| **Major Business Function** | **Enable processing of current-year budget details and future-year budget plans** | | | | |
| **System Owner**  **Phone Number** | **Sonja Strueber**  **(000) 000-0000** | | **System Administrator(s)**  **Phone Number** | | **Trunial Technologies, Inc.**  **(000) 000-0000** |
| **Data Owner(s)**  **Phone Number(s)** | **Goteti. Srinivasa Sriharsha**  **(000) 000-0000**  **Laihe song**  **(000) 000-0000** | | **Data Custodian(s)**  **Phone Number(s)** | | **Trunial Technologies, Inc.**  **(000) 000-0000** |
| **Other Relevant Information** | **BFS has been in production since May 2017** | | | | |

1. Table B: System Inventory and Definition (continued)

|  |  |
| --- | --- |
| **II. IT System Boundary and Components** | |
| **IT System Description and Components** | **BFS is a distributed client-server application transported by a network provided by PSI, a third-party. The major components of the BFS 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 BFA under contract by PSI, and this Risk Assessment relies on information regarding system hardware and Operating System software provided to BFA by PSI.**  **• One (1) network interface that is connected to BFA’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 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.**  **• 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 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.** |
| **IT System Boundary** | **• 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.**  **• 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-subdirectories: /var/opt/Oracle, /databases/Oracle, and /opt/odbc. Other directories are outside the BFS boundary.**  **• BFS is responsible for receiving data from the BCS. The BCS is a separate system and is outside the BFS boundary.**  **• 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.** |

1. 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 Budge 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** | | | | |

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.

**Figure 1: IT System Boundary Diagram**



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

1. Figure 2: Information Flow Diagram

BFS

BCS

Client

Output is stored in electronic format

and is printed for archival purposes

and includes:





Current Year Budget Details





Future Year Budget Plans

The BFS listener “listens” for client

connections on TCP port 1521 and for SCP

connections on port 22.

Budget data generated by

BCS is pushed to BFS nightly

using a cron job.

The Secure Copy Protocol

(SCP) is used to securely

perform this operation.

Users manually enter weekly and monthly budget figures. Communication to/from BFS utilizes a proprietary protocol that encrypts all data at the packet level.

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).

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**

**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.

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 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.

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.**

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 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.

2. 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.**



1. 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 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** |

1. 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** |

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.

2. 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.** | **Unauth*­­*or*­­*ized Use** | **Compromise of confiden­tial*­*ity *&* 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 of 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 *should* implement these roles *&* assign BFS privileges based on role.** |

# 

1. 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.** |

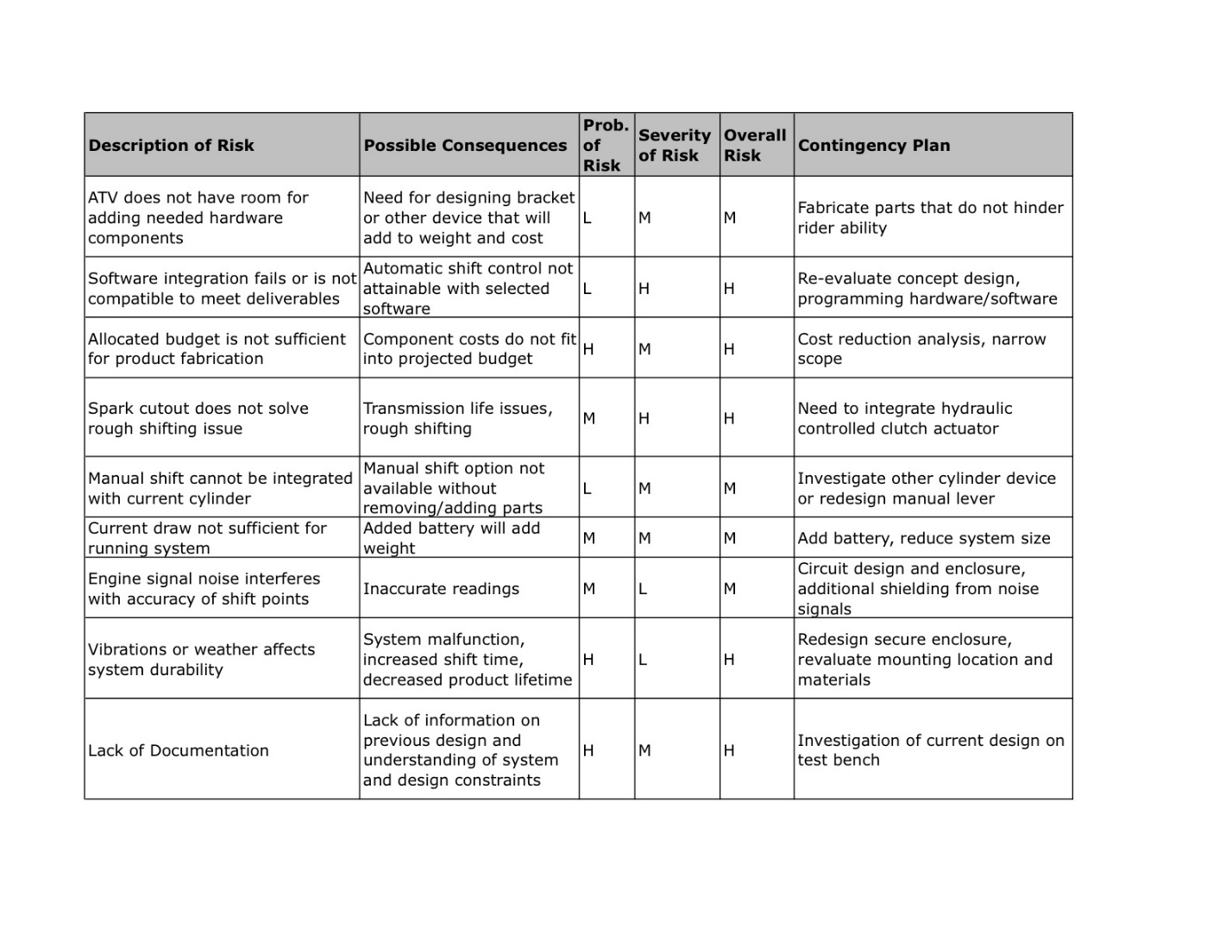
1. Exhibit 1: Risk Assessment Matrix (continued)

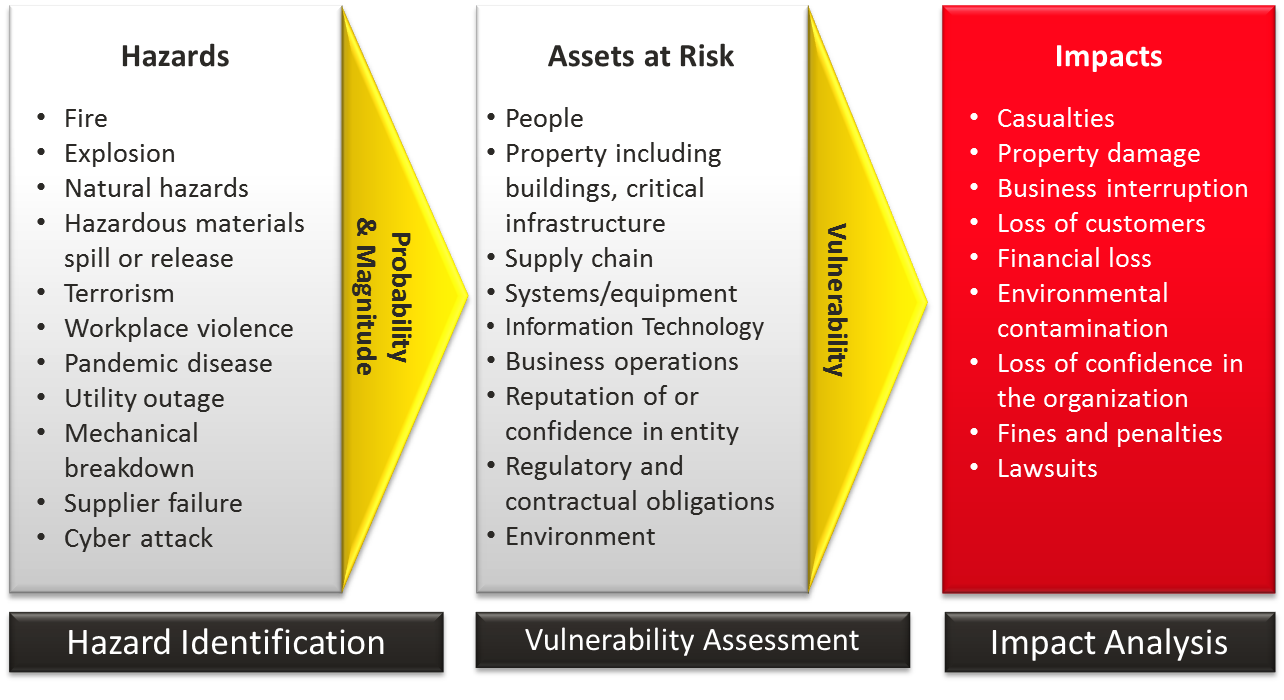
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk  No. | Vulnerability | Threat | Risk | Risk  Summary | Risk Likelihood Rating | Risk Impact Rating | Overall Risk Rating | Analysis of Relevant Controls and Other Factors | Recommendations |
| **6** | **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 created.** |

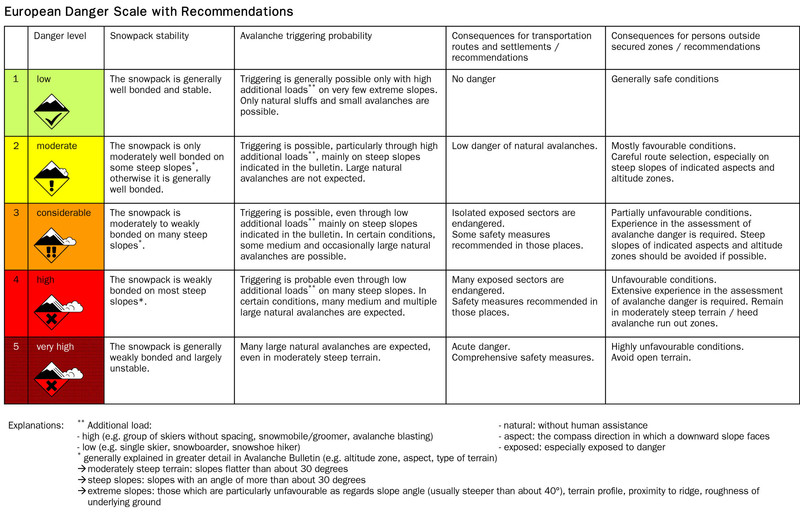
1. Exhibit 1: Risk Assessment Matrix (continued)

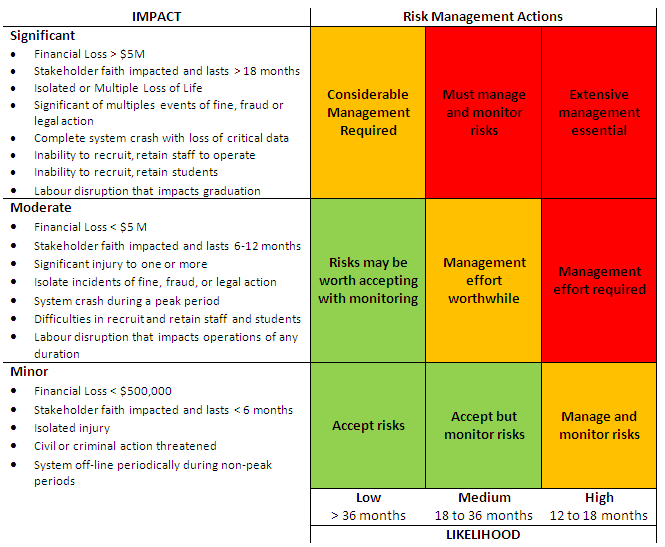
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Risk  No. | Vulnerability | Threat | Risk | Risk  Summary | Risk Likelihood Rating | Risk Impact Rating | Overall Risk Rating | Analysis of Relevant Controls and Other Factors | Recommendations |
| **9** | **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.** |

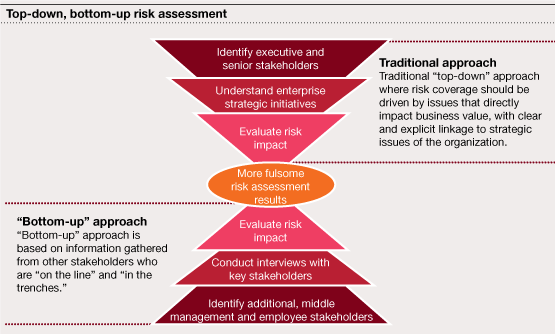
1. Use graphs to demonstrate your points.







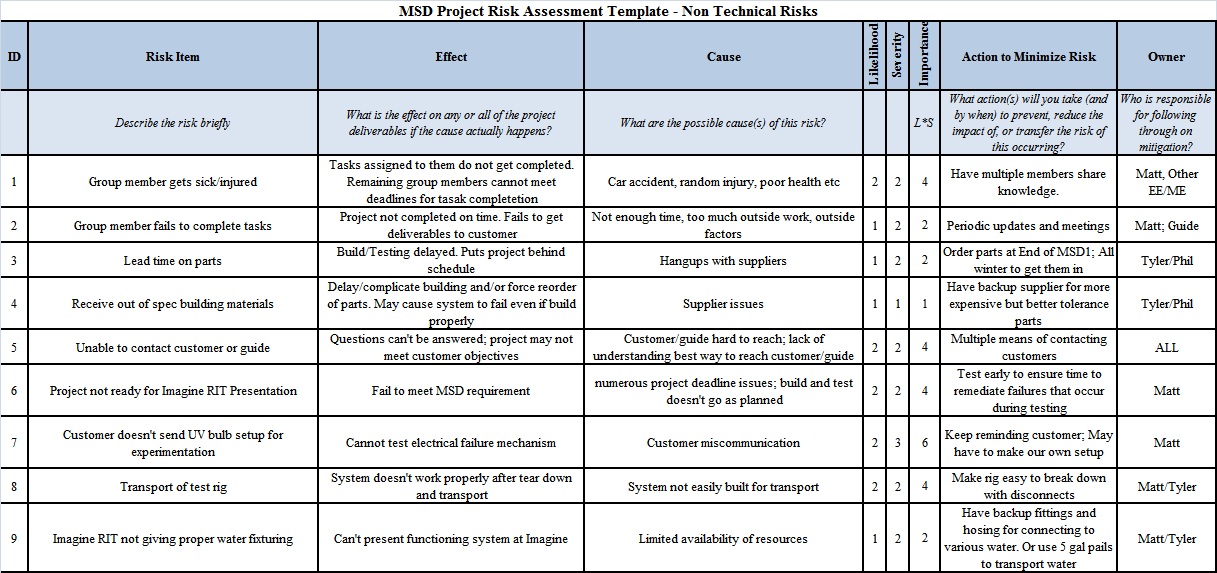


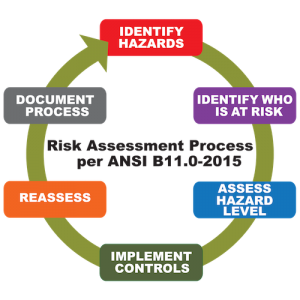


1. Compare the current status of your company with your closest competitors when possible.

We had compared our company status with other competitors one of them are GTA where we are able to satisfy the legitimate requirements of ISO Standards. As on requirement we would generally compare with others closest competitors to maintain high standards if we are missing something. Coding , Development, and gaming jumps are been identified with every risk analyze model to make it high effective in terms of standards of making earliest comparison between belonging companies.

Here is one of the graphical presentation with in the companies.





Some ancillary IT services are operated as a mix of centralized services and local support. These services include desktop support and management, file share management, print management, account provisioning, and server management. To save costs, the management of some of these services is led by administrative assistants whose primary responsibility is to support departmental administrative needs. Generally speaking, technical staff is over-worked, under paid, but is well-trained and qualified. They do their best to meet stakeholder expectations on a limited budget. The information security department split between IT Services and Service Delivery Solutions.

The company’s business and finance services are largely centralized. The administrative services component handles purchasing, physical building maintenance, and safety. HR deals with payroll, hiring procedures, and benefits. IT Services owns the Enterprise Business Systems, including HR systems, and payroll and financial systems, but Service Delivery Solutions owns all customer-focused hardware and software.

1. Research possible challenges brought up by new technologies.

**Research possible challenges brought up by new technologies.**

The application of new technology in our GreenDisk video company more and more. But these new technologies will also cause more and more potential security problems.

To reduce the most of the new technologies’ potential risks of our company, as an IT manager need to list these risks and understand of the challenges that our company and markets face.

**Cloud**

We make cloud plans to keep data and applications in-house and manage everything by ourselves. But the sensitive data store in the cloud may cause a disaster. A lot of files uploaded to cloud-based file sharing services contain sensitive data including intellectual property. When a cloud service is breached cyber criminals can gain access to this sensitive data. Absent a breach, certain services can even pose a risk if their terms and conditions claim ownership of the data uploaded to them.

**User Systems**

Desktops, laptops, notebooks, tablets and smartphones are already an integral part of many users lives. In some cases, it has become increasingly difficult to draw the line between them. The transmission of sensitive information in these devices is a potential risk. Users don’t know how to control it, may accidentally leaked sensitive information.

**Energy**

Resources and tools are readily available to help IT and data center managers benchmark energy use, identify any savings opportunities, and adopt the most energy efficient practices. Similarly, the energy is also the most dangerous and the most vulnerable to the safety in our company. The power system is destroyed or controlled by hackers can easily damage the company’s sensitive information.

**Social Networks**

Customers, suppliers and others are currently talking about our company on some form of social media. This may include Twitter, Facebook, Foursquare, LinkedIn and YouTube. At minimum, IT and marketing departments need to monitor and participate in those conversations. Semantic analysis tools can help hackers mine the information of the employees and the events of our company.

**Shadow IT**

IT continues to have a poor image inside organizations. Whether it be slow response times, dictatorial actions, or software challenges, many IT departments are facing users' preference of going to intra-department super users for help. Add the easily available cloud software and services, organizations see users and groups head toward bypassing the IT department altogether. They find and purchase third party SaaS (Software as a Service) packages to meet their needs.

Other departments like sales, marketing, accounting, etc. are considering independent arrangements with outside IT service providers. This result will lead to increased security costs and is not conducive to monitor of the IT administrator.

**BYOD and BYOA**

For years, IT has controlled user's devices. With the advent of smartphones and tablets, that has changed. Users now bring in their own devices without IT's knowledge. They use them for both personal and work-related tasks. IT's initial plan was to attempt to maintain control. The facts are clear: Controlling user-owned devices in an organization's network is nearly impossible.

When a user brings their own device, they will also bring their own applications that they have grown used to using. That is a plus for productivity and a challenge for IT security. IT managers and CIOs will need to decide what to secure: the network infrastructure or the organization's data.

1. Close with a few items proposed to improve the company’s security stance.

**Identity and Access Management:**

Greendisk will create a systematic security framework to manage electronic identities, as well as any related access permissions and ownership. This will ensure proper system usage and privileges are authenticated and administered to the correct individuals:

• Two-step password authentication will be administered for all employees.

• Three password attempts are allotted for each login session - after the failed third attempt, user accounts are then locked until the IT department can verify the user’s identity through additional security assessments.

• User passwords must be a minimum of 8 characters long, containing at least one uppercase and lower case letter, and a special character.

• Passwords will expire every 3 months. The last 10 passwords cannot be used as the new password.

• The system administrator will actively maintain the Access Control List and review list entries for each system user. The system admin will also review event and sever logs on a weekly basis to monitor potential unauthorized activity.

**Vulnerability Management:**

Greendisk will implement additional security protocols and vulnerability assessments to help ensure company assets are well-protected. The Corporate IT team will assess any changes made to IT systems and software prior to change management or release into production environments.

• A full-scope analysis must be completed in a separate test or beta environment for installation in a production environment to test any impacted security flaws, system weaknesses that can lead to backdoor entry, or any intended incompatibility or malice.

• Any noted vulnerabilities that fail the initial security assessment must be patched and mitigated before the release on the live production environment.

• If the system owner(s) notes any changes that need to be made in the production environment, approval must be received from the Corporate infrastructure team and the Chief Information Security Officer prior to any change implementation.

**Security Assessments and Management:**

• All Greendisk employees are required to complete an IT Security training program and assessment to understand company policies behind: acceptable use, password complexities, defenses against social engineering and phishing attacks through company emails.

• All Greendisk company data must be encrypted and backed-up to prevent third-party intrusions and loss of propriety information.

• Firewall and anti-virus software must be properly updated and managed. Outdated software can lead to backdoor entries and potential data breaches.

• Cloud use must be limited to Dropbox or Google Drive – all files must be password encrypted. Greendisk’s company accounts must not contain any personal user files.

References: <https://your.yale.edu/policies-procedures/policies/1614-vulnerability-management>