Jennifer Sommerfeldt
Professor David Lanter
MIS 4596 Section 1
February 1st, 2023

Risk Assessment Report 1

Executive Summary:

This report serves to analyze and evaluate the potential risks to the information stored in our financial management systems using both the NIST Special Publication 800-60 Volume II and FIPS-199. FIPS-199: "Standards for Security Categorization of Federal Information and Information Systems" and NIST Special Publication 800-60 Volume II work together to provide a comprehensive approach for conducting risk assessments of federal information and information systems. FIPS-199 provides the security impact levels for information systems, which are used to assess the overall impact of a security event on the confidentiality, integrity, and availability of the information system. NIST Special Publication 800-60 Volume II provides guidelines and recommendations for how to conduct a risk assessment of an information system. Referencing NIST, potential impacts will be categorized on the basis of confidentiality, integrity, and availability of information. The impacts are classified into three categories: low, moderate, or high, which corresponds to limited, serious, severe, or catastrophic events according to the FIPS-199 standards for security categorization of federal information and information systems.

In practice, the security impact levels established in FIPS-199 are used to determine the overall risk posed by an information system. This information, along with the guidelines and recommendations provided in NIST SP 800-60 Volume II, is used to conduct a comprehensive risk assessment of the information system. The results of the risk assessment are used to determine the appropriate security controls that need to be in place to mitigate the identified risks. Together, FIPS-199 and NIST SP 800-60 Volume II provide a consistent and systematic approach for conducting risk assessments of federal information and information systems. By using these standards and guidelines, federal agencies can better understand the potential risks to their information systems and develop effective risk management strategies.

Impact Rating Table Explained:

To summarize & conceptualize the overall effects of potential risks, an “impact rating table”, or risk assessment table is created. The table takes into account 7 key information types: asset & liability management, reporting and information, funds control, accounting, payments, collections, and receivables, and lastly cost accounting/performance measurement. Then, each information type is rated on its level of confidentiality, integrity, and availability to calculate the overall impact rating using NIST Special Publication 800-60 Volume II.

Section 1 - The Meaning and Application of Integrity, Confidentiality, and Availability:

According to FIPS 199: integrity, confidentiality, and availability are the three key aspects of information security. Integrity refers to the accuracy and consistency of information, as well as the protection of information from unauthorized modification or destruction. Confidentiality refers to the protection of information from unauthorized disclosure. Availability refers to the ability of authorized users to access information when they need it. By achieving these objectives, organizations can maintain the trust of their customers and stakeholders, protect

sensitive information from potential harm or damage, and minimize the impact of security incidents or breaches. In FIPS 199, the security impact levels for information systems are determined based on the potential adverse effects to confidentiality, integrity, and availability.

Section 2 - Security Impact Levels Explained:

The security impact levels are grouped into 3 categories: low, moderate, and high. Low indicates limited adverse effects on confidentiality, integrity, and availability. Moderate indicated serious adverse effects on confidentiality, integrity, and availability. High indicates severe or catastrophic adverse effects on confidentiality, integrity, and availability. These security impact levels provide an overall assessment of the potential consequences of a security event on the confidentiality, integrity, and availability of the information system. The security impact level is used to determine the appropriate security controls that need to be in place to mitigate the risks posed by the information system.

Impact Rating Table:

Information Type	NIST SP 800-60 ID	Confidentiality	Integrity	Availability	Overall Impact Rating
Asset and Liability Management	C.3.2.1	Low	Low	Low	**Low**
Reporting and Information	C.3.2.2	Low	Moderate	Low	**Moderate**
Funds Control	C.3.2.3	Moderate	Moderate	Low	**Moderate**
Accounting	C.3.2.4	Low	Moderate	Low	**Moderate**
Payments	C.3.2.5	Low	Moderate	Low	**Moderate**
Collections and Receivables	C.3.2.6	Low	Moderate	Low	**Moderate**
Cost Accounting/ Performance Measurement	C.3.2.7	Low	Moderate	Low	**Moderate**
	Information System Categorization:	Low	Moderate	Low	**Moderate**

Section 3 - Overall Risk Assessment & Logic:

Risk assessment is a vital component of cybersecurity that entails discovering, analyzing, and evaluating potential security threats to an organization's information systems. It is crucial to take into account various forms of information that could be at danger while doing a thorough risk assessment. As part of this, it is necessary to evaluate the security implications of various information types, including those related to asset and liability management, reporting and information, fund control, accounting information, payment information, collections and receivables, and cost accounting/performance measurement. Organizations can detect potential weaknesses and adopt the necessary security measures to guard against potential security risks by evaluating the security effect of these various forms of information. In order to protect the confidentiality, integrity, and availability of vital information systems, risk assessment is extremely important.

Asset & liability management:

The overall impact rating of asset & liability management is low due to low confidentiality, low integrity, and low availability. Unauthorized disclosure is expected to have limited adverse effects on agencies, assets, or individuals. The impact of unauthorized modification or destruction of information may depend on its urgency but is generally limited. Disruption of access to assets & liability management information is expected to have limited adverse effects on agencies, assets, or individuals due to the tolerance of delay in these processes. (NIST SP 800-60 V2)

Reporting and Information:

Financial reporting information is rated as having low confidentiality, moderate integrity, and low availability, resulting in a moderate overall impact rating as we take the highest rating per row. Unauthorized disclosure of financial information can result in limited negative effects on agency operations, assets, and individuals. Integrity issues in financial reporting can result in significant adverse effects and may lead to audits and investigations. Access disruptions to financial information are expected to have limited effects on agency operations. (NIST SP 800-60 V2)

Funds Control:

Financial reporting information is rated with low confidentiality, moderate integrity, and low availability resulting in an overall impact rating of moderate. Unauthorized disclosure of financial reporting information may have limited adverse effects on the agency, but falsified reports can lead to extensive audits and serious consequences for the agency's mission and public confidence. The integrity impact depends on the mission and data, not the time needed to detect modification or destruction, and falsified reports can have serious consequences. The availability impact depends on the mission and data, and disruptions to access are expected to have limited adverse effects on the agency. (NIST SP 800-60 V2)

Accounting Information Type:

The Accounting Information Type is rated as moderate due to its low confidentiality, moderate integrity, and low availability. Unauthorized disclosure of accounting information can cause limited adverse effects but may be serious for programs handling classified information. The integrity impact is based on the mission and its data, and small changes in data can lead to cost overruns and negative publicity. The availability impact is low, with accounting processes able to handle delays and disruptions having limited effects. (NIST SP 800-60 V2)

Payment Information:

The Payment information type is rated as moderate due to its low confidentiality, moderate integrity, and low availability. The confidentiality, integrity, and availability of payment information are evaluated based on their impact on responsible agencies. Unauthorized disclosure of payment information typically has limited adverse effects. The integrity impact level depends on the mission and data and is not time-critical. Small changes or deletions in data can result in negative publicity and corrective actions with serious adverse effects on mission functions and public confidence. The availability impact level depends on the mission and data and payment processes are generally delay-tolerant, with disruptions expected to have limited adverse effects on agency operations, assets, or individuals. (NIST SP 800-60 V2)

Collections and Receivables:

The collection and receivables information type is rated as moderate due to its low confidentiality, moderate integrity, and low availability. The confidentiality impact level refers to the harm caused by unauthorized disclosure of collections and receivables information, affecting an agency's ability to manage debts and cash receipts. Usually, this results in only limited adverse effects on operations, assets, or individuals. The integrity impact level is based on the mission and data, and small changes or deletions can cause revenue shortfalls, leading to negative publicity and affecting public confidence in the agency. The availability impact level

refers to the ease of access to collections and receivables information, which is generally tolerant of delay, causing only limited adverse effects. (NIST SP 800-60 V2)

Cost Accounting/Performance Measurement:

The cost accounting/performance measurement information type is rated as moderate due to its low confidentiality, moderate integrity, and low availability. The confidentiality impact level for cost accounting/performance measurement information is low, with unauthorized disclosure expected to have limited adverse effects on agency operations, assets, or individuals. The integrity impact level is moderate, as modifications or destruction of information can result in negative publicity and corrective actions, affecting mission functions and public confidence. The availability impact level is also low, with disruptions to access expected to have only limited adverse effects on agency operations, assets, or individuals, as cost accounting/performance measurement processes are generally tolerant of delay. (NIST SP 800-60 V2)

References

1. NIST Special Publication 800-60 Volume II
    a. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf
2. FIPS-199: “Standards for Security Categorization of Federal Information and Information Systems”
    a. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
    b. https://www.uscourts.gov/sites/default/files/fips_199_new_standards_for_security_ca_0.pdf
3. Data Classification Methodology
    a. https://portal.ct.gov/-/media/OPM/Fin-General/DataClassificationMethodology120519pdf.pdf?la=en