Data Classification Oversight and Retention Audit

Report #: 2022-05

Internal Audit

Audit Report

Sound Transit Audit Division

September 9, 2022

Sound Transit's Title VI notice of rights

Sound Transit conducts Title VI equity analyses for service and fare decisions to ensure they are made as equitably as possible.

More information on Sound Transit's Title VI notice of rights and the procedures to file a complaint may be obtained by:

- Phone: 888-889-6368; TTY Relay 711;
- Email: **stdiscriminationcomplaint@soundtransit.org**;
- Mailing to Sound Transit, Attn: Customer Service, 401 S. Jackson St. Seattle, Washington 98104-2826; or
- Visiting our offices located at 401 S. Jackson St. Seattle, Washington 98104.

A complaint may be filed directly with the Federal Transit Administration Office of Civil Rights, Attention: Complaint Team, East Building, 5th Floor – TCR, 1200 New Jersey Avenue, SE, Washington, DC 20590 or call 888-446-4511.

Report Prepared by:

This audit was initiated prepared in July 2022; however, the assigned auditor left the agency before its' conclusion and results. The Division's Deputy Director was reassigned to finalize the report.

Reviewed (QA/QC) by:

Heather F. Wright

Digitally signed by Heather F. Wright
Date: 2022.10.05 09:37:38 -06'00'

Heather Wright, Deputy Director, Audit Division

Approved for release by:

Patrick Johnson

Digitally signed by Patrick Johnson
Date: 2022.10.05 11:02:52 -07'00'

Patrick Johnson, Director, Audit Division

Table of Contents

Executive Summary

Why did we audit?

Data classification is the process of organizing information into categories that make information easy to retrieve, sort, and store for future use.

Records retention is the process of defining content as a record, then classifying and storing it for a specified amount of time.

The oversight and monitoring of these processes helps inform the agency on how we've achieved our goals, how we adhere to internal policies, and how we meet local and state regulations around the handling of our data.

The Audit Division is Sound Transit's independent assurance function that improves how the agency is operated and managed, ensuring public funds are managed transparently, and ultimately keeping employees, contractors and our riding public safe.

Effective data classification also helps to protect sensitive information, while proper records management ensures that we are being good stewards of Agency and State information.

As the agency has grown over the past 5 years, the volume of agency data has also greatly increased. This data is a valuable asset to support decision-making for operational and business transactions. Proper classification is essential in complying with information security and records management requirements to protect the agency's data and ensure accurate and reliable information is readily available to foster transparency, collaboration, and informed decision-making.

As part of our annual audit risk assessment, the process of "Data Classification, Oversight and Retention" was rated initially as an area of significant potential risk around several categories including Service Delivery, Finance, and Technology.

In our audit we focused on three specific areas of data classification: data sensitivity labelling, protection, and records retention.

There are significant risks if data is not classified appropriately, including:

- Agency restricted & sensitive data may not be properly protected from unauthorized data access, loss and misuse, and;
- Agency records may not be retained for the required length of time, leading to inefficient management of state resources.

We also noted that this audit topic aligns with Agency Strategic Goal 4.2, requiring the agency to "Establish a system that documents agency policies and procedures, tracks performance against agencywide goals and identifies and prioritizes new initiatives." Performing an audit of this area can assist the agency in assessing the degree to which this strategic goal has been achieved.

Lastly, we looked back to previous audit trends and found that four (4) prior audits: Records Management Audit (2016), IT Asset Management Audit (2019), Information Security Governance

Audit (2020), IT Access Management Audit (2021) noted similar agency-wide control issues pertaining to data classification & retention, such as:

- Unauthorized persons (e.g., terminated employee) were granted access and the access of the unauthorized persons to the data was not removed timely for the agency's systems.
- The software system inventory listing was not available at the time of the audit.
- The oversight of IT risk management was inadequate at the time of the audit.
- There was a lack of records management procedures such as inadequate metadata & classification schemes at the time of the audit.

What we found

Overall, we found the following issues:

- There are inconsistent processes for monitoring data classification and records retention;
- The agency's Data Classification Standard is compliant; however, has not been fully or consistently implemented across the agency.

Audit Process

Our audit objective was to ensure the Agency's data and information is classified, stored, and retained in compliance with applicable federal, state, and local laws and regulations, as well as with industry standards and best practices.

Through our analysis, we gained an understanding of how the agency currently classifies and retains data through the analysis of the several agency's information systems. We reviewed policies, procedures, and industry standards relating to data classification and records retention, and conducted numerous interviews with stakeholders.

Additionally, we reviewed samples of agency data to verify the data were classified and retained in compliance with Washington State's document retention schedule.

Conclusion

Based on the fieldwork reviews we performed, our audit results showed that opportunities exist to strengthen, clarify, and enhance the control environment related to data classification and records retention agency-wide.

Overall, our audit yielded only **one (1) finding** and **one (1) observation;** related to the lack of alignment in current processes and missing or incomplete portions of processes currently in place.

Remainder of this page to be left blank

1. Findings summary

The audit team completed its review and identified one (1) finding and one (1) observation, which are explained in further detail below.

This report does not include areas where procedures exist and were properly followed.

Finding 1: The Agency's Data Classification Standard has not been implemented via Agency processes and/or procedures.

Audit Risk Rating: 4C (Medium)

The agency's Data Classification and Protection Standard defines levels of data classification (restricted, sensitive, internal use, & unrestricted) for protecting the agency's data. If data is not properly classified, controls to protect sensitive and restricted data from unauthorized data access, loss, and misuse may be inaccurate, leading to a breach of information which may harm the agency.

As part of our scope, we sampled electronic and physical data stored in various agency systems and offsite storage to review how and if records were being kept according to agency policies. We requested samples of electronic data in six agency's systems. Those systems were:

- Yearli (Agency's payroll system),
- Concur (Agency's business trip system),
- Enterprise One "E1" (Agency's accounting system),
- ServiceNow (Agency's IT service and business management system),
- UltiPro Core (Agency's human resource system), and;
- QuickBase (Cloud Database).

In response to our data request, we were given a statement that the sampled data was not classified. Moreover, we were informed that among the above six systems, only Enterprise One "E1" and ServiceNow were able to classify data at the system level. QuickBase is also able to classify data at the "app" level.

We also note that this condition is primarily due to the fact that many of the agency's information systems lack the ability to apply data classification labels. Instead, we found there is a reliance on individual data users or data owners to apply these labels at the "document" level.

Additionally, there are plans to establish a Data Privacy Program to manage critical data the agency wants to protect (e.g., sensitive data); however, this program is currently on hold due to agency resource constraints. Furthermore, after reviewing selected boxes of records obtained from the storage facility, we found that none (0%) of the sampled offsite records were classified by any data classification level, to include sensitivity, due to a lack of offsite records classification labelling procedures.

Observation 1: Record retention labels are inconsistently applied

The Revised Code of Washington (RCW) 40.14 states that public records are the property of the State of Washington and do not belong to the individuals who create or receive them. Telling

Sound Transit that agency's records must be kept, managed and disposed of lawfully, according to approved state records retention schedules and according to the agency's File Plan.

In all, we sampled 60 offsite records and found that all of them were labeled and retained according to required state guidelines. However, we did note that some records were past the required retention time period and did not yet appear to be evaluated for possible destruction or archive.

During our review of the six (6) agency systems mentioned above, we also noted that there does not appear to be a retention labelling function enabled in any of them.

Positive Practices: The agency recently implemented the retention labelling function in Microsoft SharePoint in 2020, allowing the data owner to assign the appropriate retention period for each record. This function also alerts Records Management staff once a record has reached the end of its retention period.

Recommendations:

1. Conduct an evaluation of other systems to verify if the retention label function is available.

2. Continue training and education across the Agency to remind employees that records retention labeling technology is only effective when individuals consistently use it.

2. Approach to This Audit

To comprehensively evaluate data classification oversight and retention, we looked at regulations, standards and best practices and compared them to the current state including internal policies, procedures, and records. ST Performance Auditors progressed through the following phases to arrive at this final report:

Phase 1: Planning, Scope and Objectives

To identify the risks and controls related to the data classification and retention process, as well as determine the audit objectives and scope; we performed the following steps:

- We reviewed policies, procedures, and industry standards to gain the understanding of the data classification and retention process**;**
- We performed an analysis of the agency's file plan to identify all records of departments and their retention period.
- We performed an analysis of the agency's systems required to establish an audit population for testing against audit criteria.
- Lastly, we gained an understanding of the data classification and retention process for the selected system owners in the agency systems.

Our audit scope included all data and records in the Agency's acceptable storage systems, and offsite storage locations. We also took into consideration agency policies, procedures, and standards related to Data Classification Oversight and Retention.

The objective of the audit was to evaluate agency criteria to ensure data and information is classified, stored, and retained according to industry standards.

To do so, we wanted to determine whether the agency has effective controls to classify, store and retain data and information in compliance with the agency policies and procedures; and we wanted to determine whether the agency's data and information policies and procedures align with applicable regulatory requirements and industry standards.

Phase 2: Field Work & Reporting

During field work, auditors performed a number of tests to determine whether the agency has effective controls to classify, store and retain the electronic data in the agency's systems and offsite records in compliance with the agency policies and procedures.

We requested ten (10) electronic data sets within six selected agency systems. The selection of these systems was based on our initial risk assessment of data classification and retention. Also, we generated a random sample size of 60 offsite records. Based on the audit procedures applied, we verified the following related to the management of data classification and retention:

- Proper data classification categories (restricted, sensitive, internal use, unrestricted) for each data and record;
- Proper retention label for each data and record based on agency's file plan;
- The agency's data classification and protection standard is aligned with applicable regulatory requirements and industry standards.

The results of our assessment informed our audit conclusions and the associated findings and observations.

Based on the details of our testing obtained during field work, we can show where risks were not adequately mitigated. Please refer to Section 4, "Analysis" for further details.

Audit Division Standards

The Audit Division conducted this work under the framework outlined in its charter. It governed itself adhering to the mandatory elements of The Institute of Internal Auditors' (IIA) International Professional Practices Framework (IPPF or "Red Book"), including the Core Principles for the Professional Practice of Internal Auditing, the Code of Ethics, the International Standards for the Professional Practice of Internal Auditing (the Standards), and the Definition of Internal Auditing.

The division conducts audits in accordance with Generally Accepted Government Auditing Standards (GAGAS or "Yellow Book") promulgated by the United States Government Accountability Office (GAO).

Additionally, the Audit Division is also committed to following safety oversight standards set forth by the Federal Transit Administration (FTA), Federal Railroad Administration (FRA); as well as all other relevant requirements or standards for auditing.

3. Background

Sound Transit generates significant amounts of data to plan, execute, and improve its operations. Data classification processes are essential to maintaining the data in the agency's system and ensure its integrity, protection, and accessibility. The agency recognized the important its data classification, and the division of Information Technology, Information Security (InfoSec.) has established the data classification and protection standard (Version 2.2 September 2021: most recent version).

This standard defines the roles and responsibilities for data user, owners, and custodian, four data classification levels (unrestricted, internal use, sensitive, & restricted), and data protection guidelines including the data storage locations.

It states that the system custodian is responsible for maintaining systems or methods to store information/data. The data user and owners are responsible for the label data classification. In addition, InfoSec. is responsible for oversight the agency's information security.

Additionally, the division of Strategic Business Services Office (SBS), Records Management, is the responsible authority for Agency Policy 2000, which provides the guidelines for maintaining data. Moreover, the Records Management division maintains our own internal guidance, known as the agency file plan, and sets the records retention schedule for the agency's data based on Washington States' retention guidelines.

The agency's file plan is not a compliance standard, but rather is a list of records that refer to a disposition authority number (or DAN for short) indicating what should be kept, how long they should be kept, and when can they be dispositioned for archive.

Records management also ensures agency records are managed according to the retention schedule.

Currently, approximately 400 software and systems are in use agency-wide; with records being created and stored by each department/division in a number of decentralized data storage locations (or systems).

Some examples of acceptable data storage locations are network storage locations, offsite storage, SharePoint, and the Sound Transit website (The Hub).

There are locations not acceptable for the retaining of the public records. Those are 1) the systems not under the custodianship of Sound Transit IT such as cloud-based services, 2) devices personally owned desktop computer, tablets, mobile phones, and 3) removable media (e.g., thumb drives, external hard drives)

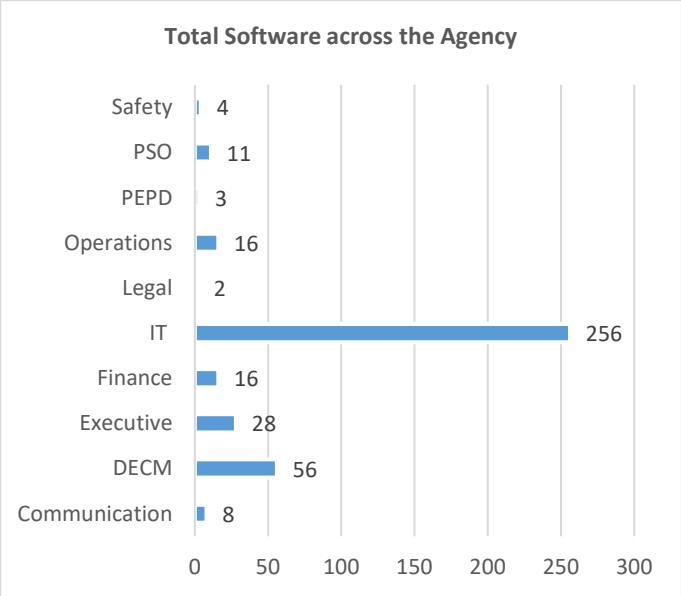

Figure 1: Total software systems (Agency)

Our audit analyzed that approximately 20% (80 of the nearly 400 software and systems) may contain agency's data, as shown above in Figure 1. The remaining 80% of the software is used for supporting and creating the agency's data. Additionally, 36% of the software systems are either internet-based systems or on-premises systems solely owned and managed by the business unit; with the remaining 64% managed and maintained by IT.

For the past few years, the agency has been steadily working to better manage and house its' data. Starting in 2019, there has been a push to migrate agency electronic data from SharePoint 2010 to MS 365 SharePoint. This migration is scheduled to complete later this year and will improve data management including adhering to agency and state data classification and retention schedules.

Records Management division is also conducting training on the functionality to the divisions that complete the migration of data.

Remainder of this page to be left blank

For offsite storage, the agency (Records Management) has a process for storing hard copy records in an offsite location.

The description of records is documented in the inventory form including the classification of records, and Records Management verifies the inventory form is complete and the records are properly packed in standard record storage boxes prior to shipping to offsite storage.

Records Management evaluates records eligible for disposition on an annual basis, in coordination with the record owner.

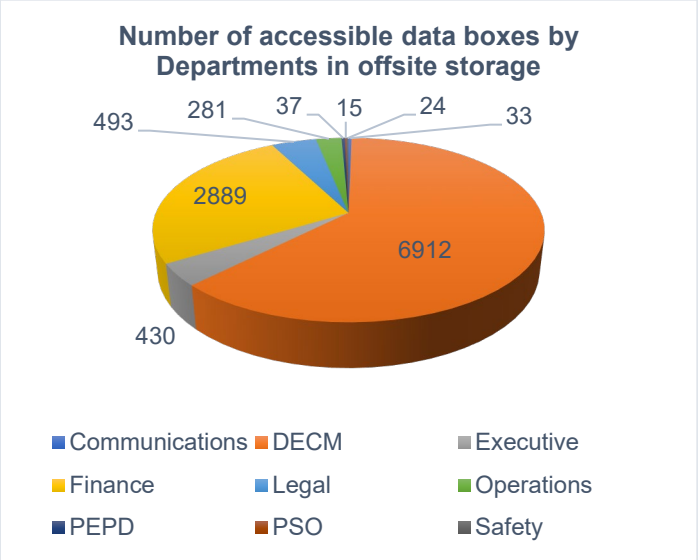

Figure 2: Graph of accessible data records (Offsite)

The archival records after the evaluation by Records Management will be retained permanently or transferred to the Washington State Archives for preservation. Records not eligible for archive, that meet the retention period and are no longer needed for the agency business will be securely destroyed after the evaluation.

Currently, over 11,100 boxes of accessible records are stored in the offsite storage facility, as represented by the chart. Of the 11,100, 6,912 (62%) of the boxes stored come from DECM, and 2,889 (26%) are pertinent to Finance.

The records management division evaluates both electronic and physical records, to ensure these records meet retention periods based in the state retention schedules, and determines the final disposition and transferring of records for the archival phase.

Based on the sensitivity level, agency data is classified into the following four (4) data classification levels:

- Restricted;
- Sensitive;
- Internal Use;
- Unrestricted

The following table below explains in more detail what each classification level is, and some examples of that data.

Data classification level	Data classification Definition	Examples of data (not limited to)
Restricted	Extremely sensitive information and has strict handling requirements per state or federal statues, regulations or Sound Transit Contract	• Credit Card or Debit Card Numbers • Sensitive Security Information • Personally Identifying Information (PII) belonging to certain nonagency personnel (e.g. ORCA customers) • Information related to Fire, Life and Safety Systems • Information with contractual requirements for protections above the standard "Sensitive" and "Internal Use" controls • Medical files and records(PHI) • Investigation records • Attorney-Client Communications
Sensitive	Information that requires special handling above the standard protections given to most information handled by Sound Transit.	• Personally Identifying Information (PII) • IT infrastructure and security configuration diagrams • Passwords and similar credentials (unless associated to a system that processes "Restricted" data, in which case, these credentials would also be "Restricted") • Payroll Information • Investigation Reports (Legal and HR)
Internal Use	All information created and used by ST that does not fall under any other category. Internal Use data is the majority of Sound Transit data and not shared freely with the Public.	• Grant Agreements • Executed MOUs • Org Charts • Training Materials • Scorecards • Inter Office Communications • Internal Financial Statements • Draft Audit Reports • Communication / Marketing Plans • Policies and Standards • Press Releases in draft version • Design documentation
Unrestricted	Data explicitly intended for public consumption in final version	• Press/News Releases • Job Descriptions • Final Audit Reports • Budget Books • Social Media Content

Table 1: Data Classification levels, definitions and examples

Remainder of this page to be left blank

4. Diversity, Equity, and Inclusion Review

Throughout our audit, we utilized a diversity, equity, and inclusion (DEI) lens to consider the context of how data is being classified, maintained, retained or destroyed; asking the question; "Are we (Sound Transit) consistently applying the data classification and protection standard to all employees for creating records.

While we recognize that data classification and retention is an agency-wide function, there's room for improvement on how we classify, retain, and protect agency data as we become an anti-racist organization. Strong considerations should be looked into for improving and enhancing how we ensure DEI data is retained and protected, who will have access to that data, and who will be responsible for stored and disposed of properly.

5. Conclusion & Recommendations

Overall, our audit identified that while we have robust procedures, processes, and standards, they have not been fully implemented across all divisions and/or departments.

Audit requests that management address the one (1) finding, and consider the following recommendations to improve processes and reduce risks:

- Develop and implement a classification method for each record location or system in accordance with the Data Classification and Protection Standard.
    - Evaluate the function of the label data classification for each agency system and consider implementing the tool for labelling classification for the agency systems.
    - Enhance data classification procedures to include classification labelling of offsite records
    - Create and maintain an inventory of data in the agency's systems, especially sensitive and restricted records.
- Enhance the evaluation process of electronic data and offsite records for the archive phase (e.g., preserve or destroy records).
- Update and clarify which positions within departments are responsible for the roles and responsibilities in the data classification and protection standard
- Update and clarify the IT risk assessment process

Management Response

Prepared by: Kathy Albert Chief Strategic Business Officer and Jason Weiss, Chief Information Officer

Date: September 30, 2022

Audit: Data Classification, Monitoring and Retention (AUD-PA-2022-05)

Management Response:

Management agrees with the audit report finding.

Finding 1: The Agency's Data Classification Standard has not been implemented via Agency processes and/or procedures.
Audit Risk Rating: *4C (Medium)*

Management Response / Action Plan:

Thank you for the opportunity to provide a management response to the Data Classification, Monitoring, and Retention audit. Management agrees with the finding. The Strategic Business Services office in partnership with Information Technology (IT), will develop a strategic vision for data classification, that will seek to address the core issues identified in this audit finding. Implementation of the vision will be accomplished in partnership with all Agency functions, and through a structured, managed programmatic approach with senior leadership oversight.

Timeline for corrective action:

The Strategic Business Services office and IT intend to reach substantial completion of its strategic vision in approximately one year. Additional implementation details will be defined at that time and will include the overall prioritization of the Data Classification effort, and available resources.

Prepared by: Michele Hanrahan, Director - Records Management

Date: September 27, 2022

Audit: Data Classification, Monitoring and Retention (AUD-PA-2022-05)

Observation 1: Record retention labels are inconsistently applied

Management Response:

Management agrees with the audit report observation as pertaining to electronic records. The agency has implemented systems and processes for the labeling of electronic records in SharePoint to enable their retention and disposition and maintains a roadmap for evaluating other systems to verify if the retention label function is available. The report validates and supports the actions management has taken to date.

While the report notes on page 8 that some paper records were past the required retention period and did not yet appear to be evaluated for disposition, the agency has fully implemented an annual disposition process through which evaluation of paper records does occur. In some cases, the decision to retain records beyond the required minimum retention period is made by the record owner. Washington State requirements include ensuring public records are not inappropriately destroyed; are retained for minimum requirements (if not longer according to business requirements); and meeting public information records requests. While the current practices have met the Washington State requirements, we agree that retaining records beyond the minimum required length of time may lead to increased storage costs and reduced efficiency.

Action Plan:

- The report's recommendations are in line with management's road map for the continued implementation of record retention labeling within agency systems that allow for such configuration, starting with applications within the Microsoft 365 platform.

- Systems containing structured data will be evaluated for their record retention labeling capabilities.

- Agency-wide training to increase awareness of responsibilities is an ongoing practice which includes quarterly live training sessions and a self-serve online module.

Appendix A: Audit Finding Risk Rating Process

To aid process owners in prioritization of the audit findings resulting from the audit, a level of audit risk will be assigned by assessing two factors: 1.) the probability that the associated problem will occur at some point in the future, and 2.) the impact or severity of that problem in relation to the overall business process.

Using the same Risk Assessment Matrix already in used throughout the agency and based on the MIL-STD-882-E; audit findings are qualitatively assessed based on the worst credible case that is anticipated from the result of human error, design inadequacies, component failure or a malfunction.

Risk Rating Scale

	Severity	Catastrophic (1)	Critical (2)	Major (3)	Marginal (4)	Negligible (5)
Probability	Frequent (A)	High (1A)	High (2A)	High (3A)	Serious (4A)	Medium (5A)
	Probable (B)	High (1B)	High (2B)	Serious (3B)	Serious (4B)	Medium (5B)
	Occasional (C)	High (1C)	Serious (2C)	Serious (3C)	Medium (4C)	Low (5C)
	Remote (D)	Serious (1D)	Medium (2D)	Medium (3D)	Low (4D)	Low (5D)
	Improbable (E)	Medium (1E)	Medium (2E)	Low (3E)	Low (4E)	Low (5E)
	Eliminated (F)	**Eliminated**				

Resolution Requirements

Risk Score	Risk Level	Risk Rating	Minimum Actions	Risk Acceptance / Responsibility
1A, 1B, 1C, 2A, 2B, 3A	High	Unacceptable	Stop work & immediate correction required to reduce risk.	Not Acceptable. Executive Team is informed.
1D, 2C, 3B, 3C, 4A, 4B	Serious	Undesirable	Mitigation strategy required to reduce risk within 30 days of identification of risk.	Acceptable with risk controls and monitoring. Director-level committee review and approval.
1E, 2D, 2E, 3D, 4C, 5A, 5B	Medium	Acceptable w/ review	Monitor and consider actions to further reduce risks.	Acceptable with risk controls and monitoring. Technical Level committee review and approval.
3E, 4D, 4E, 5C, 5D, 5E	Low	Acceptable	Acceptable without further mitigation. May be accepted by the business unit in coordination with Audit and Safety.	Acceptable without further mitigation. May be acceptable by the business unit with coordination with Audit and Safety.
N/A	Eliminated	Eliminated	No actions needed.	N/A

Risk Matrices

Severity	Catastrophic (1)	Critical (2)	Major (3)	Marginal (4)	Negligible (5)
System Disruption / Operations	> 24 hrs Substantial or total loss of operations	12 – 24 hrs Partial shutdown of operation	4 – 12 hrs Prolonged disruption of operations	1 – 4 hrs Brief disruption of operations	<1 hour Minor to No disruption
Financial	>$5,000,000	$1,000,000 – 4,999,999	$249,999 – 999,999	$10,000 – 249,999	< $10,000
Reputational	Prolonged negative media coverage for >30 days and / or irreparable reputational damage, resulting in government intervention	Ongoing negative media coverage for >14 days but ≤ 30 days causing serious reputational damage, resulting in government intervention.	Ongoing negative media coverage >7 days but ≤14, causing major reputational damage and possible government intervention	Ongoing negative media coverage for ≥ 24 hours but ≤ 7 days, causing some reputational damage	Negative media coverage for ≤ 24 hours, causing minor reputational damage
Injury	Several deaths (≥3) and / or numerous (≥3) serious injuries (excluding suicides or by natural causes)	1 -2 deaths and/or 2 or more serious injuries	Multiple minor injuries and possible serious injury (Ambulance transport)	Minor injury such as bruising, abrasions, bleeding; possible medical services required	No injuries
Equipment	Total loss of equipment or system interruption requiring more than 30 days to repair.	Significant loss of equipment or system interruption requiring more than 14 days but less than 30 days to repair.	Some loss of equipment or system interruption requiring more than 24 hours but less than 14 days to repair.	Minor system loss of equipment or system interruption requiring less than 24 hours to repair.	Minor damage to equipment or minor system interruption with no immediate repair necessary.
Regulatory	Cease and desist orders are delivered by regulators. Critical assets and facilities are forced by regulators to be shut down.	Governmental, regulator investigations, and enforcement actions, lasting longer than a year. Violations that result in multiple large non-financial sanctions; **OR** Regulators force the removal and replacement of management positions. Regulators begin agency monitoring activities.	Violations that result in significant fines or penalties above and beyond what is codified or a regulator enforces non-financial sanctions; **OR** Significant new and updated regulations are enacted as a result of an event.	Violations that result in fines or penalties	Self-reported or regulator identified violations with no fines or penalties

Probability Level	Likelihood of event in specific item	MTBE in Operating Hours **	Occurrence in time
Frequent (A)	Will occur frequently.	<1,000 oh	1 per week, likely to occur several times per month
Probable (B)	Will occur several times.	1,000 – 100,000 oh	1 per month, likely to occur several times per year
Occasional (C)	Likely to occur sometime.	100,000 – 1,000,000 oh	Once per year, likely to occur several times within 10 years
Remote (D)	Unlikely but possible to occur.	1,000,000 – 100,000,000 oh	1 per 10 years or likely to occur several times within 100 years
Improbable (E)	So unlikely, occur may not be experienced.	>100,000,000 oh	1 per 100 years
Eliminated (F)	Risk removed / eliminated	Never	N/A