SOUNDTRANSIT

Audit Report

Business Continuity & Disaster Recovery Audit

Report Number: 2021 - 01 | Report Date: May 13, 2021

Executive Summary

Audit Report No.: 2021 – 01 **May 13, 2021**

WE AUDITED the current Business Continuity & Disaster Recovery processes to ensure agency on-going monitoring controls spanning over 'business critical' functions and our critical IT systems.

While the Audit Division's other audit function (Compliance Audit group) canvas' Emergency Management as a function of system safety across all modes, this audit looks deeper at processes to ensure good controls are in place surrounding the BCDR process as a whole.

Our **AUDIT OBJECTIVES** were to determine whether Sound Transit has effective controls in place over BCDR processes to ensure:

- Adequate continuity of operations planning for major events.
- Business Impact Analysis for essential functions are effectively and routinely performed to ensure agency preparedness and appropriate recovery strategies.

The audit examined documents and processes in place from January 1, 2019 to March 15, 2021.

DocuSigned by:
Patrick Johnson
D893DEC00D0B4A6...

Patrick Johnson
Director, Audit Division

WHAT WE FOUND?

Sound Transit (ST or agency) recognizes that there are wide-ranging emergency and disaster situations that can impact the agency's ability to provide safe and secure transit services. Thus, the agency is committed to increasing its resiliency through advanced preparation and operational recovery in an organized and coordinated manner. Consistent with applicable policies and regulations, the agency has established an Emergency Management (EM) program (under ST Public Safety) to administer an effective emergency response involving: (1) External partners (e.g., operating, jurisdictional, county, and state response agencies) and (2) key ST divisions.

As part of its overall Emergency Management Plan (EMP), ST's EM Division works to coordinate and prepare the agency for potential disruptive events, disasters, recovery efforts, and restoration of services. This is accomplished under a Continuity of Operations Plan (COOP), to ensure the continuation of essential agency functions, and enable a rapid response to any emergency situation. As of March 2021, there are an estimated 38 COOP plans (active or archived) reflective of ST's organizational structure. Of the 38, 14 (or 37%) of those plans were available at the time of our review.

Business Continuity & Disaster Recovery

Business Continuity includes disaster planning that provides a road map to ensure agency essential functions continue and restore operations while minimizing damages and losses.

Sound Transit's approach to BCDR is decentralized (by design) wherein certain activities (e.g., updated essential information, trainings, etc.) are dispersed to individual departments and system owners. Two key divisions consisting of EM and Information Security (InfoSec) separately oversee and manage aspects of BCDR including: (1) business continuity planning; and (2) technical recoverability of critical systems, respectively.

Conclusion: During our review, while we observed that the agency has incorporated certain essential features of BCDR (e.g., dedicated staffing, enhanced 'Safety and Security' assessments, etc.), we identified **one finding related to strengthening monitoring controls**. These controls include ensuring: (1) agency-level and division-specific COOPs are updated, maintained, and tested; and (2) the preceding plans are adequately guided by a comprehensive Business Impact Analysis process.

Table of Contents

Background

Sound Transit (ST or agency) recognizes that there are wide-ranging emergency and disaster situations that can impact the agency's ability to provide safe and secure transit services. While the majority of these events cannot be prevented, Sound Transit is committed to increasing agency's resilience through advanced preparation and operational recovery in an organized and coordinated manner. Consistent with applicable policies and regulations[1], the agency has established an Emergency Management (EM) Division (under ST Public Safety) to administer an effective emergency response involving: (1) External partners (e.g., operating, jurisdictional, county, and state response agencies) and (2) key ST divisions.

As part of its overall Emergency Management Plan (EMP), ST's EM Division works to coordinate and prepare the agency for potential disruptive events, disasters, recovery efforts, and restoration of services. This is accomplished under a Continuity of Operations Plan (COOP).[2] As of March 2021, there are an estimated 38 COOP plans (active or archived) reflective of ST's organizational structure. Of the 38, 14 (or 37%) of those plans were available at the time of our review.

Business Continuity & Disaster Recovery (BCDR)

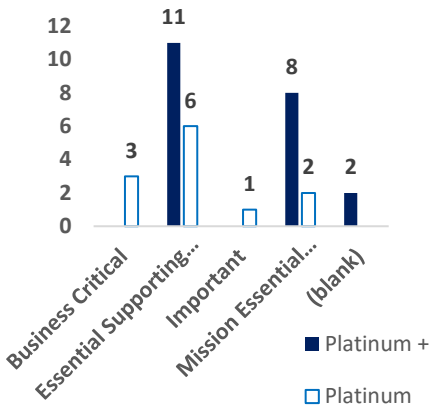
Business Continuity includes disaster planning that provides a road map to ensure agency essential functions continue and restore operations while minimizing damages and losses. Of the areas related to BCDR, we focused primarily on on-going monitoring controls spanning both 'business critical' functions and IT systems for adequate audit coverage.[3] Sound Transit's approach to BCDR is decentralized (by design) wherein certain activities (e.g., updated essential information, trainings, etc.) are dispersed to individual departments and system owners. Two key divisions, EM and Information Security (InfoSec), separately oversee and manage aspects of BCDR including: (1) business continuity planning (BCP); and (2) technical recoverability of critical systems, respectively.

During our review, InfoSec identified approximately 89 total systems[4] agency-wide. Of the 89, 57 (or 64%) of those were assessed as high criticality rating consisting of 33 (or 37%) "Platinum Tier"; and 24 (or 27%) "Gold Tier".

[1] Board Resolution No. R2017-14 Adopting a Security, Law Enforcement, and Emergency Management Plan.
[2] EM defines COOP as an effort within individual organizations to ensure that Primary Mission Essential Functions continue to be performed during a wide range of emergencies.
[3] In alignment with Internal Auditing standards, Auditors have increased coordination activities and reliance with Audit Division's Compliance Program. Compliance Audit Group performs on-going modal safety audits (including EM & Preparedness Program). Refer to **'Scope and Methodology' section** for more details.
[4] During the course of our audit, one additional Platinum + was subsequently identified as part of the TR list.

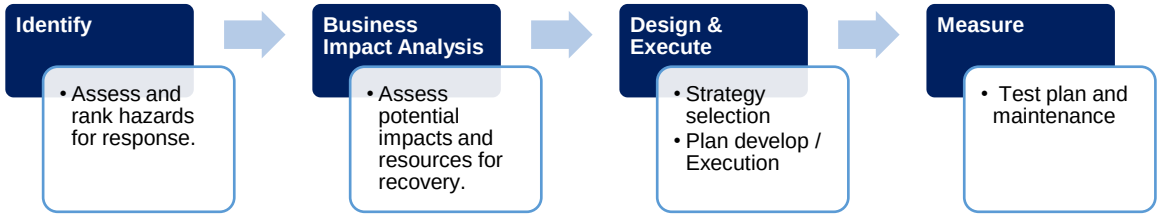
Category	Count of Systems (by Tier)					Total
	Silver	Platinum +	Platinum	Gold	Bronze	
Business Critical	2		3	6		**11**
Essential Supporting Activity	13	11	6	14	3	**47**
Important	12		1	4	2	**19**
Mission Essential Function		8	2			**10**
(blank) [1]		2				**2**
Grand Total	**27**	**21**	**12**	**24**	**5**	**89**

Summary of Criticality Controls Matrix			
Criticality		Loss Type	
Agency Impact	Risk Tier	RTO	RPO
Catastrophic 5	Platinum +	4 Hrs.	24 Hrs.
Critical 4	Platinum	24 Hrs.	24 Hrs.
Major 3	Gold	72 Hrs.	24 Hrs.
Marginal 2	Silver	1 week	48 Hrs.
Insignificant 1	Bronze	> 1 Month	1 week



AD prepared (source: InfoSec TR Listing & STTR Manual).
[1] Note: Line item was categorized as 'blank' as this was part of general testing related ST's core infrastructure.

Per agency guidance (e.g., EMP and Technology Resilience manual), BCP begins with an understanding and analysis of threats, vulnerabilities and likelihood also known as the 'all-hazards approach'. This process requires a business impact analysis[5], which identifies key essential functions, operations, and critical systems as a precursor to recovery strategies. The final output is (1) formal division-specific plans and (2) an agency COOP ('living' document[6]). Monitoring controls include ensuring preceding plans are subject to periodic updates; and recurring trainings, tests and exercises (TTE).



AD prepared (source: EMP 2014 and audit walkthroughs)

EM and InfoSec are primarily reportable to internal oversight bodies contained within each division. Specifically, InfoSec reports to the newly established Information Security Risk Council as the primary governing body.[7] Additionally, escalation mechanisms exist for EM

[5] Business Impact Analysis (BIA): An analysis conducted within each department with the aim of identifying functions that are essential to agency operation. The Business Impact Analysis differentiates **essential functions** from those that are non-essential to the **immediate continuity of business**.
[6] Due to the nature of their criticality, "Living Documents" are key documents that are continually updated as business conditions change.
[7] Audit Division's InfoSec Governance Audit Report No: 2020-04 (dated, 07/13/20) found areas of improvement related to enhancing the agency's overall information security oversight process. As part of our follow-recommendation process, early planning work to include Executive Sponsorship for the establishment of the Risk Charter, identification of Council Members, quarterly meetings, etc. were implemented as of October 2020.

(as part of Public Safety) through numerous Safety & Security Committees (e.g., Safety and Security Operations Committee).

Moreover, both divisions are subjected to independent reviews regarding BCDR. InfoSec facilitates scheduled external assessments to determine that the agency's information systems and security posture conforms to industry standards (i.e., ISO 27000 series controls); and 'EM & Preparedness Program' is continuously reviewed by the Audit Division's Compliance Audit Group (Modal Safety Audits) as required by applicable state and federal regulations.[8]

Audit Objectives

To determine whether Sound Transit has effective controls in place over Business Continuity & Disaster Recovery processes to ensure:

- Adequate continuity of operations planning for major events.
- Business Impact Analysis for essential functions are effectively and routinely performed to ensure agency preparedness and appropriate recovery strategies.

Scope and Methodology

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained, and reported upon below provides a reasonable basis for our findings and conclusions based on our audit objectives.

Over the course of the audit, we gained an understanding of the BCDR process at the agency, department and division levels through data analysis, observation, documentation reviews, and personnel interviews. We identified risks in the processes and assessed management controls in place to mitigate those risks. Based on our assessment of management control effectiveness, we focused on controls over the agency's process related to: (1) adequate continuity of operations planning for major events; and (2) effective and routine Business Impact Analyses to ensure agency preparedness and appropriate recovery strategies.

Audit reviewed plans, policies, processes, procedures and reports for the period January 1, 2019 through March 15, 2021.

[8] Modal Safety Audits – As required by 49 CFR 673, the WSDOT Rail Safety Oversight Program Standard and APTA's Recommended Guidance for Internal Safety Oversight of Commuter Rail requiring ST to perform annual, ongoing internal safety audits to ensure the agency is effectively implementing Agency Safety and Model Safety Program Plans. Refer to **Audit Division 2021~2023 Agency Audit Plan** (link) for more details.

Objective 1:

To determine whether Sound Transit has effective controls in place over BCDR processes to ensure adequate continuity of operations planning for major events, we performed the following procedures:

1. Performed comprehensive examinations of applicable policies, procedures, and standards to gain a sufficient understanding of the audit environment. Audit also reviewed prior audits in developing and ascertaining areas of high risk.[9]
2. Selected 14 of 38 (or 37%) available COOP plans & related archives with additional audit emphasis into 4 selected plans representing 'critical business functions'.[10]
    a. Basis of selection were derived from, but not limited to: preliminary stakeholder questionnaires/interviews [11] , areas of significant risk and availability of documentation stored in current repositories and prior cloud-based program[12].
    b. Coordinated interviews and process walkthroughs to determine if controls were working effectively as intended.
        i. Individuals interviewed included Director of Public Safety, Director Transportation Safety & Security, Deputy Director-Emergency Management, Deputy Director-Public Safety, EM Specialist, Disaster Recovery Administrator, Director of FP&A and Budget, Manager – Health and Safety, and Senior Business Analyst.
    c. Examined division-specific plans and supporting documentation to determine if plans were sufficiently developed, up-to-date, and tested in accordance with requirements. Key records reviewed included an estimated 16 source documents for each areas selected spanning essential functions, facilities, TTEs, etc.

Objective 2:

To determine whether Sound Transit has effective controls in place over BCDR processes to ensure business impact analysis for essential functions are effectively and routinely performed to ensure agency preparedness and appropriate recovery strategies, we performed the following procedures:

1. Analyzed the agency's primary methods of Business Impact Analysis (for Public Safety and InfoSec) against selected attributes to determine whether business impact analyses are routinely performed. These were comprised of:

[9] Audit criteria consisted of the following: **(1) Agency plans and procedures** (e.g., Resolution R2017-14, EMP 2014 (rev. 1, dated 08/14), EMP 2020 (rev. 2, dated 02/20), etc.; and **(1) standards** (e.g., APTA Standards for Emergency Management & Continuity of Operations, ISO 27001 Information Security Framework, etc.). Prior audit coverage included: **(1) Internal** (i.e., ST Maturity Assessment: IT [dated, 06/15]; Safety Assurance Audit [dated, 05/20]; and Information Security Governance Audit [dated, 07/20]; AD Annual Internal Safety Audit Tacoma Link Light Rail [dated, 12/20]; and AD Annual Internal Safety Audit Sounder Commuter Rail [dated, 01/21]) and **(2) External** (i.e., ST InfoSec Maturity Compliance Assessment Report [dated, 10/20]; and Link Light Rail Operations Technology Assessment [02/20]).

[10] Audit sampling unit: Emergency Management, Facilities, Finance – Payroll, and Human Resources.

[11] As part of its prelim survey, control questionnaires in conjunction with interviews were used to assess seven key areas including: (1) Management support; (2) Risk assessment & mitigation; (3) Business Impact Analysis; (4) Business Continuity and (5) Recovery Strategy; (6) Plan Awareness & training; and (7) maintenance.

[12] Sound Transit previously utilized software and cloud-based document repository to manage COOP Plans.

   a. **Public Safety:** Hazard Identification and Risk Assessment (HIRA); and Threat and Vulnerability Assessment (TVA).
   b. **InfoSec:** System Effect Analysis (SEA).
2. Selected 5 of 89 (or 6%) total systems for limited review to determine the adequacy of controls in place and to the degree which they meet SEA requirements. Basis of judgmental selection included criticality rating ("Platinum +")[13], complexity, etc.
   a. Key supporting documentation reviewed included: SEA Questionnaires, Sound Transit Technology Resilience (STTR) Maturity Scorecard, TR system list and analysis, TR roadmap, Disaster Recovery Runbook, STTR exercise framework, tabletop exercises (e.g., Operations Technology Failover Tabletop Summary Report), ST Cybersecurity Incident Response Plan, etc.

Conclusion

During our review, while we observed that the agency had incorporated certain essential features of BCDR, we identified **one finding related to the strengthening of monitoring controls**. These included ensuring: (1) agency-level and division-specific COOPs are updated, maintained, and tested; and (2) the preceding plans are adequately guided by a comprehensive business impact analysis process (i.e., complete identification of essential functions and information systems that support those functions).

Notable areas of progression towards implementing an agency-wide COOP program included:

- Dedicated staffing (i.e., EM Specialist and DR Administrator);
- Critical systems have been analyzed and rated for criticality;
- Ongoing-efforts to conduct site recovery plans and tabletop testing; and
- Enhanced TVA process including consolidation of 'safety and security' assessments (embedded control) with the goal of creating data-driven mitigation plans.

Our audit did find opportunities for improvement related to COOP practices that would enable the agency to handle continuity and recovery situations more effectively. While management continues to maintain a decentralized approach (by design), we recommend the agency strengthen its impact analysis process (at the appropriate level) thereby enhancing recovery strategies to reflect current conditions and prioritization.

Moreover, streamline inefficiencies through centralization of EM's system of records and formalize series of guidance documents (e.g., EMP, COOP, etc.) as agency-level policies to facilitate a strong control environment.

[13] Coordinated with management to determine the appropriateness of Sensitive Security Information (SSI) in line with the agency's 'Data Classification and Protection Standard (dated, 03/28/17).'

Findings and Recommendations

1. Agency's Business Continuity Planning Process must be Strengthened, Enhanced and Tested

The Audit Division completed its review over the agency's BCDR processes. Based on our examination, we found opportunities of improvement related to enhancing monitoring controls to ensure: (1) agency-level and division-specific COOPs are updated, maintained, and tested; and (2) the preceding plans are adequately guided by a comprehensive business impact analysis process.

For the period examined, the agency estimated a total of 38 participating departments and corresponding plans[14]; and 89 enterprise level systems within the agency, and 57 of those were considered critical, requiring recovery within three days or less. From the population derived, we examined 14 available divisional archives; and performed a limited review of 5 additional critical systems to determine the adequacy of controls over BCDR activities.

Additional consideration was given when determining the appropriateness of audit criteria for evaluation. Audit notes that in August 2014, EM established a comprehensive plan delineating in detail the requirements of a business impact analysis and COOP process known as the Emergency Management Plan (EMP). Recently, in February 2020, the EMP was revised and a significant portion of preceding controls were removed.[15] Thus, conditions within the performance period (or audit scope 2019 through 2021) were evaluated concurrently against criteria from the 2014 and 2020 revisions of the EMP and Sound Transit Technology Resilience (STTR) manual.

Based on our audit testing and fieldwork procedures, specific exceptions were noted as follows:

Emergency Management

- Overall, the agency lacks an overarching COOP plan (informed by a business impact analysis process) per EMP 2014 section 8.6.1(a). Audit notes while this was superseded by EMP 2020 (issued in 02/20), a 'BCP plan' (or agency-COOP) should have been in place for the period examined.
- 24 of 38 (or 63%) participating divisions did not have indication of any COOP plans and supporting documentation (e.g., business impact analyses, essential worksheets, etc.) stored within EM's repository.
- For the remaining 14 (or 36%) plans and EM archives reviewed, we found COOPs were not updated since 2018 and a majority of delegated training, testing, and exercises (TTEs) have ceased since 2017. Auditor's note that recent migration efforts from a prior third-party platform was a contributing factor to the lack of records on file.

[14] During the course of our audit, EM estimated 38 participating departments and corresponding plans as part of its 'draft COOP' guidance. The population of 38 COOP plans was corroborated with key staff and verified against repositories.
[15] EMP 2020 omitted business impact analysis component; and defined COOP requirements related to ST Express. Audit notes the document is absent references to relevant agency policies or documents.

Information Security

- Despite efforts to complete system assessments and testing, contingency planning remains challenged as **the process does not align to prioritized key essential functions to support recovery efforts**. Management noted that prioritization and alignment is dependent on a reliable business impact analysis and technical guidance required at the divisional-level to ensure COOPs contained informed inputs.
- Within the period examined, InfoSec identified 89 systems reviewed for impact. Of those 89, 57 were rated as Gold and above. Of those 57 Gold+, 14 (or 24%) have documented ISCPs. The remaining 43 (or 75%) are still a work-in-progress and slated for completion in Q4 2021.

In our opinion, the overall conditions occurred due to: (1) overreliance on two divisional key process owners[16] to manage agency's BCDR functions (EM and InfoSec) as a program; (2) process inefficiencies (inadequate communication protocol, underutilized central repository, numerous templates, etc.); and (3) unauthorized plans at the appropriate level of detail to facilitate a strong control environment.

As a result, there is limited assurance that agency employees and management (e.g., assigned planners, key contacts, successors, etc.) are aware of department COOP protocol and can access such plans in the event of a major disruption. Additionally, lacking a business impact analysis process further diminishes the agency's preparedness in identifying and prioritizing key essential functions & information (e.g., recovery time, alternate facilities, additional resources, etc.).

1) Strengthen Monitoring and Documentary Controls over Agency's COOP Process

Consistent with APTA standards[17], ST's EM coordinates the development of a Continuity of Operations Plan (COOP)[18] – at both the divisional-specific and agency-level. Key elements of these plans include:

- Identification of key staff/human capital.
- A list of essential functions and services provided by each organization of Sound Transit has been arranged in order of priority is documented in their respective COOP's and identifies the essential functions operations.
- A list of vital records and resources including databases and systems.
- Periods of time for which and after which disruptions could result in significant losses to Sound Transit.
- Training and exercises performed to maintain an accurate and effective continuity & recovery strategy.

[16] Audit notes that as of March 2021, two dedicated staffing resources comprised of one EM specialist; and one InfoSec DR Administrator have since been assigned to spearhead business and IT systems (agency-wide), respectively.
[17] Standard for a Continuity of Operations Plan for Transit Agencies.
[18] Continuity of Operations: An effort within individual organizations to ensure that Primary Mission Essential Functions (MEF)s continue to be performed during a wide range of emergencies.

EMP 2014 section 8.6.1(a)-(b) further requires the activation of an overall Business Continuity Plan (BCP) during a level 1 emergency (e.g., major fire, pandemic, etc.), affecting the entire agency with a potential for lasting at least two weeks.

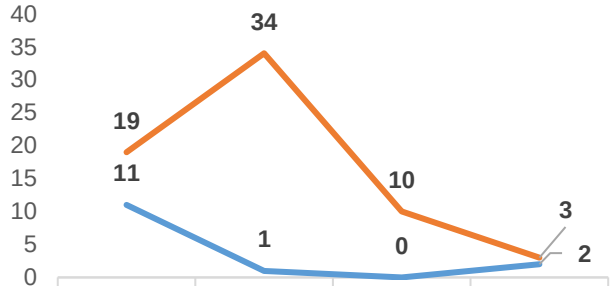
Audit performed testing for a sample of 14 (of 38 total) available divisional COOP plans with additional audit emphasis into 4 specific plans[19] for completeness. Based on examination of EM's system of records and audit procedures applied, we found the following general areas of improvement:

- Overall, the agency lacks an overarching COOP plan (informed by a business impact analysis process) contrary to EMP 2014 section 8.6.1(a). Audit notes while EMP 2014 was superseded by EMP 2020 (issued on 02/20), a BCP plan should have been in place for the period examined.
- 24 of 38 (or 63%) identified participating areas did not have any indication of COOP plans and supporting documentation (e.g., business impact analyses) within the repository. This was primarily due to recent migration efforts from a prior third-party platform and inadequate participation by assigned continuity planners (per division) to ensure timely updates.[20]

Of the remaining 14 (or 37%) plans and available archives, we found the following:

- All division-specific plans on file were last dated for August 2018 or earlier and do not have indication of 'records of change' for monitoring and tracking. Additionally, while DR component for IT is managed separately, ISCPs – similar to a division-specific COOP – are slated to be completed in 2021 (refer to **next section**).
- Examination of training & exercise schedules (to exclude IT) revealed that majority of trainings (e.g., tabletops) for the remaining individual divisions have not occurred since 2017 (EMP section 6.2).

See **Table** below for Count of Trainings and Login.



	FY 2017	FY 2018	FY 2019	FY 2020
Count Training	11	1	0	2
Count Login	19	34	10	3

AD prepared (source: EM repository and division TTEs).

[19] Additional sampling unit included Emergency Management, Facilities, Finance – Payroll, and Human Resources.
[20] Sound Transit previously utilized software and cloud-based document repository to manage COOP Plans.

Note: During the course of our audit, management had indicated that the preceding initiatives were ceased due to increased cost and overall lack of value-added. This resulted in migration efforts of all vital records from the prior platform to agency's SharePoint.

The conditions above occurred due to unauthorized policies and plans (at the appropriate level of authority) to administer staff participation coupled with process inefficiencies such as utilization of lengthy plans for the intended divisions. Further analysis of migrated files revealed divisions were using approx. 16 templates in their continuity planning, which resulted in an overall reduction of login activities since 2019 (or approx. 84% decline) within the three year period examined.

Furthermore, although one key process owner has been assigned to manage continuity planning agency-wide (prior and current implementation), it was also asserted that limited resources continue to be constrained by higher-level priorities, i.e., interfacing with external entities within the region (e.g., transit partners and other response agencies).

2) Plans should be Adequately Guided by a Business Impact Analysis Process

R2017-14[21] sections 2.1 to 2.2 enhances the agency's commitment to providing a safe and secure environment for passengers, employees, contractors, emergency responders and the public. Consistent with Board Policy and APTA standards, EMP 2014 sections 3, 4, and 8 indicates BCP begins with an understanding and analysis of threats (e.g., natural, human-caused, and technological), vulnerabilities and likelihood. This should be followed by a business impact analysis inclusive of the following elements:

- Identifying essential functions, operations, and processes for each department.
- Estimating the potential impact for each essential function, assuming worst-case scenarios.
- Prioritizing the effort for recovery of the essential functions.
- Identifying the resources required to recover and resume the essential functions, operations, and processes.

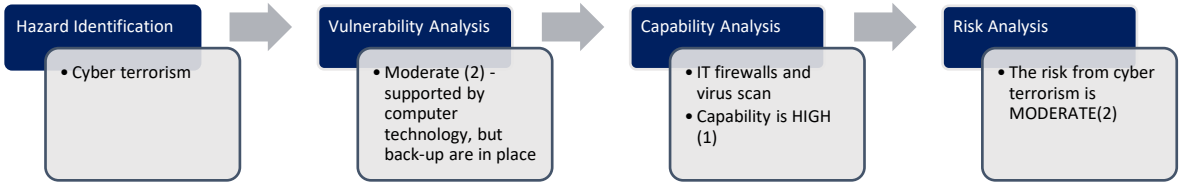
Section 8.5 indicates each department/division is required to conduct a business impact analysis for their units and incorporated as part of the COOP.

Subsequent assessment of hazards that can cause emergencies and disasters should be used to rank and prioritize agency planning and response. Interviews with management specified two primary methods for performing an overall impact analysis comprised of the (1) HIRA (outsourced to partnering transit agencies [dated July 2019]); and (2) Threat Vulnerability Assessments (TVAs).[22] See **Diagrams** to the right and below.

	EMP 2014	Hazard Ranking		HIRA (dated, July 2019)	Hazard Ranking
1	**Earthquake**	High	1	Cyber	High
2	**Cyber**	Moderate	2	Pandemic Flu	High
3	Adverse Weather	Moderate	3	Transportation Accident	High
4	Flood	Moderate	4	Earthquake	High
5	Bomb Threat	Moderate	5	Terrorism	High
6	Chemical/radiological	Moderate			
7	**Terrorism WMD**	Moderate			
8	Landslide	Moderate			
9	Fire	Moderate			
10	Volcano	Low			
11	Workplace Violence	Low			
12	**Pandemic Flu**	Low			

[21] Resolution No. R2017-14 (dated, 04/17) section 2.2 requires agency's programs to maintain risk, threat and vulnerability identification, analysis and evaluation activities to eliminate or mitigate risks and liability […].
[22] Interviews with Sr. Management indicated that THIRA / HIVA / TVA / HIRA are used interchangeably.

Impact Analysis & Hazards Response (Sample – Cyber Terrorism)



AD prepared (source: EMP 2014 and HIRA 2019).

For the purposes of our audit, we reviewed key supporting documentation (e.g., essential worksheets) and archives to determine the existence and occurrence of a business impact analysis process (foundation). Based on our examination and audit procedures applied, **we found the agency does not routinely perform business impact analyses consistent with agency processes.** Specific exceptions are as follows:

- While the EMP 2014 incorporated an agency-level business impact analysis, it was noted that all but one of the 38 areas (i.e., IT) did not have updated documentation on file evidencing the furtherance of a business impact analysis process since the file migration in 2018. We noted that the requirement of performing an impact analysis was omitted in the current EMP 2020 (issued on 02/20).
    - Although key information relative to division-specific business impact analyses were stored for 14 of the 38 plans prior to the 2018 cutoff, the remaining areas could not be validated due to lack of documentation.
- While HIRA and TVAs were referenced as the agency's preferred methods to performing its impact analysis, there appears to be no clear linkage to BCP methods (e.g., summary of hazards ranking, specific hazard response, etc.) that would inform recovery strategies.

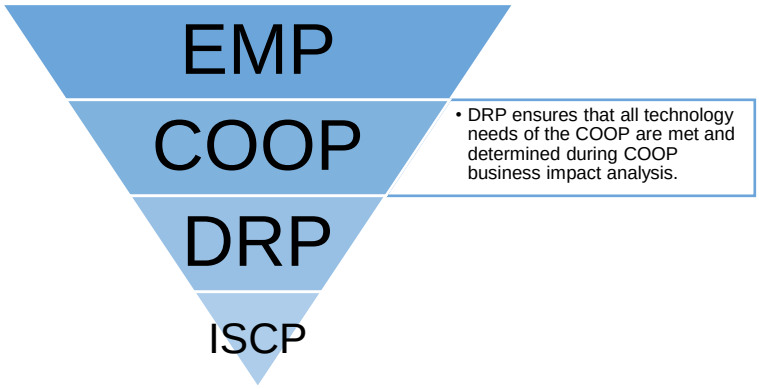
The conditions above occurred because plans and processes emphasizing routine performance of business impact analyses were not followed by designated staff. Barring an effective business impact analysis process that prioritizes recovery efforts of essential functions, there is an increased risk that COOP plans may be ineffective in the resumption of key operations.

Strengthen Coordination of Contingency and Recovery Planning Efforts

EMP 2020 section 3.9 indicates that the IT department will be responsible for: (1) assessing IT infrastructure and applications that are impacted by an incident; and (2) restore communications, technology equipment, systems, and/or data per defined recovery point objectives and service levels.

STTR Standard (dated, 12/20) sections 2.1 & 2.3 prescribes IT contingency and recovery efforts process steps and documentation. The process begins with an evaluation of potential impacts through the System Effect Analysis (SEA), requiring each system to be analyzed for the risks they pose. Criticality ratings are assigned to assist in prioritization of recovery activities and are based on a five tier rating scale (e.g., Platinum +, gold, etc.). Evaluation factors include life and safety of individuals, essential functions, etc.

Final results are documented as part of ISCP – a detailed profile including shutdown, failover, and reconstitution procedures, as well a stakeholder contact and communications. Tasks from the ISCP and corresponding instructions are sequenced in the Disaster Recovery Plan (DRP) [23] and should be incorporated as part of the agency-COOP (as a key aspect). See **Diagram to the right**.



Source: STTR (dated, 12/20)

Based on our review of control documentation and analysis obtained, we noted the following:

- Despite efforts to complete system assessments and testing, contingency planning remains challenged as **the process does not align to prioritized key essential functions to support recovery efforts**. Management noted that prioritization and alignment is dependent on a reliable business impact analysis and technical guidance required at the divisional-level to ensure COOPs contained informed inputs.
- Within the period examined, InfoSec identified 89 systems reviewed for impact. Of those 89, 57 were rated as Gold and above. Of those 57 Gold+, 14 (or 24%) have documented ISCPs. The remaining 43 (or 75%) are still a work-in-progress and slated for completion in Q4 2021.

Audit observed controls (i.e., SEAs, tabletop exercises, and DRPs) were 'functioning and present' through additional risk-based testing of five selected systems categorized as Platinum+ (see **table below**).

	Rating	Category	BIA Completion Date	Tier	Plan Required?
1	5.1	Mission Essential Function	6/17/2020	Platinum +	Yes
2	4.8	Mission Essential Function	2/10/2021	Platinum +	Yes
3	4.8	Essential Supporting Activity	2/10/2021	Platinum +	Yes
4	4.5	Mission Essential Function	6/17/2020	Platinum +	Yes
5	4.02	Mission Essential Function	6/17/2020	Platinum +	Yes

AD prepared (Source: InfoSec TR listing).
Note: Sensitive information was removed.[24]

[23] DRP is a broad technology plan to recover all critical information systems at a secondary location (physical or virtual). Comprised of multiple ISCP's sequenced appropriately (e.g., networks before servers and MEF supporting systems before ESA supporting systems). DRP activates during a severe disruption to core technology infrastructure or loss of site.
[24] For more information regarding risk details, InfoSec is available, as needed.

Overall, the conditions above occurred due to the inadequate information and communication protocol that would integrate key essential functions to DR component (i.e., systems recovery of those functions). Additionally, it was noted that ST has no authoritative and informed prioritized key essential functions list. Essential worksheets were maintained as part of the divisional COOP process up until 2018; however, the process was not guided by a sufficient impact analysis (recovery time, recovery objectives, etc.) that would increase the reliability of inputs & incorporate associated mapping of key activities required to support systems recovery of those functions.

Furthermore, we noted one DR Administrator is responsible for managing, coordinating, and hosting tabletop exercises for 89 related systems. A review of recent (1) external and (2) internal assessments (i.e., 'TR maturity scorecard') yielded 'adequacy rates' of 64%[25] and 61%, respectively. However, interim meetings with key staff also indicated that more systems have been identified since our initial engagement, potentially increasing further delays in achieving programmatic objectives (e.g., ISCPs tentative for Q4 2021).

Recommendations

Managing an effective BCDR program at Sound Transit is an agency-wide effort, often requiring the support of senior management and right level of oversight. Documented and approved policies should clearly delineate the chain of accountability over the COOP and DR process, and specify ownership of individual plans within each department & division.

Thus, to enhance controls over the business continuity planning process, we recommend Emergency Management Division, in collaboration with pertinent senior management, to implement the following:

1. Accelerate efforts to officially ratify EM's series of guidance (e.g., EMP, Continuity of Operations [COOP] guidance, etc.) at the appropriate level to facilitate a stronger control environment.
2. Re-assess policies with an emphasis in formalizing monitoring and communication controls. Key considerations are as follows:
    - Leveraging cross-divisional continuity teams and establish periodic meetings (as indicated in the COOP guidance). Focused training and technical assistance covering COOP developments, business impact analyses, etc. should be provided while ensuring plans contain key essential elements (at the appropriate level of detail).
    - BCDR efforts and high-level issues should be tracked and reportable to existing oversight bodies (e.g., Risk Committee) for increased accountability.
3. Streamline process inefficiencies including:
    - Establishing a central repository (via SharePoint) for visibility and

[25] ST InfoSec Maturity Compliance Assessment Report (dated, 10/20) rated information security continuity as 3.2 out of 5 (or 64%). External assessors concluded the process is 'defined' and well within industry standards.

maintenance. Appropriate access in line with agency policy[26] should be provided to 'continuity planners' (per division) in ensuring COOPs (division-specific and agency-level), analysis, and vital records are kept current.

- Consolidate essential worksheets (e.g., master worksheet) for simplification of data entries for key divisions. Information can be updated by assigned continuity planners and prompted by EM Specialist, as-needed.

Management Response:

Prepared by: David Wright, Chief Safety Officer
Date: September 7, 2021
Audit: Business Continuity & Disaster Planning Audit

Management Response:

Finding 1: Agency's Business Continuity planning process must be strengthened, enhanced, and tested

- Strengthen monitoring and documentary controls of Agency's COOP process
- Plans should be adequately guided by a business impact analysis process

Management Response / Action Plan: Management **partially agrees** with the audit finding identified in this report.

In early 2020, Emergency Management (EM) initiated an agency-wide outreach to review and update Continuity of Operations Plan (COOP) documents. They (EM) intended to engage with our internal stakeholders and provide further education and awareness of COOP planning and the need to add/update Division plan information as appropriate.

However, those priorities shifted due to the agency's response to the worldwide COVID-19 pandemic. It was, and remains, EM's top priority to continue to improve the role of the Division COOP in the agency's response to disruptive incidents and ensure continuity of service.

We learned through the pandemic that the process to update and roll out agency-wide COOP changes requires us to 'individualize' our approach. This new process will allow our team to provide informational sessions, provide feedback to Divisions, and facilitate the update of division and department plans; as well as provide clarity as part of a larger COOP.

[26] User permissions and permission levels (e.g., limited access) via SharePoint server may be granted to key users in line with agency's Data Classification and Protection Standard and in consultation with ST's Records Management.

This will increase plan consistency across the agency, further educate staff on the fundamental information necessary for COOP, and streamline the process to update annually.

While the Business Impact Analysis process was listed in a previous Emergency Management Plan, EM team members do not have the training or knowledge to implement this process. Instead, EM team members found that the use of the Hazard Identification and Risk Assessment (HIRA) methodology has been more appropriate for a regional transit authority than a Business Impact Analysis. Therefore, the Business Impact Analysis section was removed, and team members have used HIRA documentation to inform COOP development.

EM provides an overview of the COOP development process and our HIRA to our stakeholders at update meetings. This HIRA is completed in conjunction with local county officials to identify county-level hazards and risks that may impact our operations. Currently, Sound Transit has a completed HIRA for Pierce County, with the King County assessment in its final stages - the HIRA for Snohomish County is planned for 2022. It is these identified hazards that EM discusses with our stakeholders to drive their COOP planning. EM has and will continue to use these documents to identify potential incidents that could impact operations within each Division.

EM will continue our coordination with IT SecOps for recovery planning efforts during our quarterly meetings. In these meetings, we review current progress on our COOP plans, IT Disaster Recovery (DR) plans, identify efforts to align our practices, and opportunities to increase collaboration. Additionally, these meetings provide opportunities to increase communications and information sharing between the two units and other stakeholders.

EM **agrees** with the overarching recommendation to support agency-wide shared ownership of COOP. The end goal is an effective BCDR process cannot have EM, nor IT as the sponsor. Every department and division in the agency must take responsibility and accountability for their plans. While EM and IT (DR) should be included as facilitators and subject matter experts, agency-wide involvement is critical for a robust and coordinated COOP – ultimately increasing or agency's resilience and adaptability.

Lastly, EM **disagrees** with the recommendation of establishing a central repository for visibility and maintenance of plans, as this is an item that is outside of our purview. This is an item neither EM nor IT can control nor has responsibility for. Document control and management is, and has been, an agency-wide issue - so much so that Agency Strategic Priority #4 focuses on transforming and unifying core agency business processes, to include creating a system that documents agency policies and procedures, this plan should be included there.

Timeline for corrective action:

Item 1 – COOP resumption/agency support: We are currently finalizing the schedule for the resumption of COOP plan review and will begin that process around Q3 2021.

COOP Repository: EM does not believe the recommendation for establishing a central repository for visibility and maintenance of plans falls within our responsibility. Therefore, there is neither an actionable resolution nor timeline.

Item 2 - Business Impact Analysis: EM has integrated a review of our current identified vulnerabilities into our initial department/division roll out meetings. Each draft plan will be reviewed with these hazards in mind to ensure functional plans are established to address the risks.