ASIS - Business Continuity and Disaster Recovery Policy

Contents

Aviation Safety Technology

Satisfies	TSC:
	- CC5.1
	- CC7.5
	- CC9.1

Version:	1.0
Date:	09 Feb 22

Change / Revision Record

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete reissue of the entire document.

Version	Date	Change/Revision Description
1.0	09 Feb 2023	Initial Document

1 Overview

Business systems are vital to the Aviation Safety Technology Division's (organization) mission/business processes; therefore, it is critical that services provided by the organziation are able to operate effectively without excessive interruption. The organization's Business Continuity Plan, which is stored in Alfresco along with all security-related documents, establishes the overall plan for implementing Business Continuation (BCP/Contingency Planning (CP) and Disaster Recovery (DR) and comprehensive procedures to support the organization quickly and effectively following a service disruption to normal operations.

The Aviation Safety Information System (ASIS) is hosted by AWS, and the AWS uptime exceeds the service-level standard supported by ASIS. Hazards associated with AWS outages are separated based on severity. By default, ASIS is deployed in the US East (NorVA) region. ASIS maintains a warm backup site in the US West (NorCal) region, with backups in both the US East and US West regions. Offline backups are transferred to rsync.net and stored independently of AWS. See Reference 5A.

2 Purpose

This policy includes an overview of continuity operations, outlines the approach for supporting an organization's critical business functions, and defines the roles and responsibilities of staff. This document also outlines the orders of succession, notification procedures and communication methods, and the plan for maintaining and restoring access to vital records.

3 Scope

This policy applies to all

a. Infrastructure and data within the organization's information security program.

b. Management, employees, and suppliers that are involved in decisions and processes affecting the organization's business continuity. This policy must be made readily available to all whom it applies to.

4 Background

a. The success of the organization is reliant upon the preservation of critical business operations and essential functions used to deliver key products and services. The purpose of this policy is to define the criteria for continuing business operations for the organization in the event of a disruption. Specifically, this document defines:

   i. The structure and authority to ensure business resilience of key processes and systems.

   ii. The requirements for efforts to manage through a disaster or other disruptive event when the need arises.

   iii. The criteria to efficiently and effectively resume normal business operations after a disruption.

b. Within this document, the following definitions apply:

   i. *Business impact analysis/assessment* - an exercise that determines the impact of losing the support of any resource to an enterprise, establishes the escalation of that loss over time, identifies the minimum resources needed to return to a normal level of operation, and prioritizes recovery of processes and the supporting system.

   ii. *Disaster recovery plan* - a set of human, physical, technical, and procedural resources to return to a normal level of operation, within a defined time and cost, when an activity is interrupted by an emergency or disaster.

iii. *Recovery time objective* - the amount of time allowed for the recovery of a business function or resource to a normal level after a disaster or disruption occurs.

iv. *Recovery point objective* - determined based on the acceptable data loss in the case of disruption of operations.

5 References

a. Reference A: ASIS Backup and Recovery Policy

6 Policy

6.1 Business Risk Assessment and Business Impact Analysis

a. Each Program Manager is required to assist the organization Vice President in developing a business risk assessment and business impact analysis for area of responsibility.

b. The business risk assessment must identify and define the criticality of key business systems and the repositories that contain the relevant and necessary data for the key business system.

c. The business risk assessment must define and document the Disaster Recovery Plan (DRP) for their area of responsibility. The DRP shall include:

1. Key business processes.
2. Applicable risk to availability.
3. Prioritization of recovery.
4. Recovery Time Objectives (RTOs).
5. Recovery Point Objectives (RPOs).

6.2 Disaster Recovery Plan

a. The organization must have a documented DRP to provide guidance when hardware, software, or networks become critically dysfunctional or cease to function (short and long term outages).

b. The DRP must include an explanation of the magnitude of information or system unavailability in the event of an outage and the process that would be implemented to continue business operations during the outage. Where feasible, the DRP must consider the use of alternative, off-site computer operations (cold, warm, hot sites).

c. The plan must be reviewed against the organization's strategy, objectives, culture, and ethics, as well as policy, legal, statutory and regulatory requirements.

d. The DRP must include:

1. An emergency mode operations plan for continuing operations in the event of temporary hardware, software, or network outages.
2. A recovery plan for returning business functions and services to normal on-site operations.
3. Procedures for periodic testing, review, and revisions of the DRP for all affected business systems, as a group and/or individually.

6.3 Data Backup and Restoration Plans

a. The ASIS Backup and Recovery Policy provides policy and guidance for backup and recovery operation (Reference 3A)

b. A backup restoration test is performed monthly during the xxxx (waitingforDuane)

6.4 Risk Assessment

The following table reflects hazard probability assumptions for the Business Continuity Plan:

Table 1: Risk Assessment

Hazard	Probability	Magnitude	Warning	Duration	Risk Priority	Mitigation
Short-term Disruption in service in US East	Low	Limited	None	< 24 Hours	High	Allow AWS to correct their issues.
Long-term Disruption in service in US East	Low	Critical	None	< 4 Days	Medium	Move operations to US West. The procedures to perform this operation are in the *ASIS Disaster Recovery Plan*.
Termination of AWS due to national natural disaster	Extremely Low	Catastrophic	None	> 4 Days	Low	This is the only hazard in AWS that would lead to complete disruption of our services for an extended period of time. Due to the nature of this type of hazard and the impact that this will have on all our customers, independent of our system, the recovery plan in this situation will be to set up a new hosting facility in the USA using the offsite backups of all critical ASIS data stored at rsync.net. Validation of these offsite backups are part of the disaster recovery procedures.
Disruption in Podio	Low	Limited	None	> 1 Day	Low	Podio is used internally to support project management and online collaboration between ASIS Team members as well as to document policy and procedures. If there is a disruption in service, the team can use alternative tools (such as Office365), and Slack can be used to support this functionality. In the event of a disruption in service, the mitigation plan is to allow Podio to correct their issues.
Disruption in rsync.net	Low	Limited	None	> 1 Day	Low	Offsite backups are maintained by rsync.net. while primary backups are stored in AWS. Therefore, a disruption in service will not impact ASIS. rsync.net self-hosts, and data is archived completely independent of AWS. In the event of a disruption in service, the mitigation plan is to allow rsync.net to correct their issues.

Risk Assessment						
Hazard	**Probability**	**Magnitude**	**Warning**	**Duration**	**Risk Priority**	**Mitigation**
Disruption in Zendesk	Low	Limited	None	> 1 Day	Low	Zendesk is our primary tool to support customer service. During a disruption in service, the ASIS Support Team has contact information for our customers in Podio and Mail Chimp, a third-party broadcast email service. In the event of a disruption in service, the mitigation plan is to allow Zendesk to correct their issues.
Disruption in Slack	Low	Limited	None	> 1 Day	Low	Slack is used internally for communication (similar to SMS) between ASIS team members. The *Aviation Safety Contact List* contains email addresses, postal addresses, and phone numbers for the entire team. The contents of this list can be used with alternative commination tools (such as email and Podio) to support this functionality during an interruption in service. In the event of a disruption in service, the mitigation plan is to allow Slack to correct their issues.
Disruption in Alfresco	Low	Limited	None	> 1 Day	Low	Alfresco is an open-source document management tool that ASIS hosts using AWS. No hazard is associated with a disruption in this service. In the event of a disruption in service, ASIS will implement the *Information System Contingency Plan*.
Disruption in Subversion	Low	Limited	None	> 1 Day	Low	Subversion is an open-source version control system supporting the maintenance, development, and operations of the ASIS information systems. In the event of a disruption in service, ASIS will implement the *Information System Contingency Plan*.

6.5 Critical Business Function

a. The critical business function of ASIS is to maintain services to customers as defined in the service-level standard in the WBAT Software and Related Services Agreement (excerpt in Table 2). Software development, while integral to operations, is not a critical business function.

b. A risk assessment associated with the critical business function is listed in Table 1.

6.6 Maintain Service-Level Standard

a. ASIS's capability to achieve its critical business function relies on the AWS Infrastructure as a Service (IaaS) and Zendesk. ASIS will make all reasonable efforts to ensure all ASIS-maintained sites support at least 99.5% uptime, which does not include scheduled downtime for maintenance as coordinated with the customer.

b. The ASIS Support Team's primary responsibilities are defined in Table 2 "Expected Actions".

Table 2: Service-Level Standard		
Severity Level	**Minimum Response**	**Expected Action**
Severity Level 1 – Application is unusable or a breach in security has occurred.	< 1 day	Severity Level 1 problems shall have someone assigned to fix the issue within 16 hours and, if possible, a patch for the fix ready for implementation into production. If a patch is not ready by the 24th hour, an estimate will be provided to the customer.
Severity Level 2 – Application is usable but fails intermittently or inhibits the user's ability to function.	< 3 days	Severity Level 2 problems shall have someone assigned to fix the issue within 72 hours and, if possible, a patch for the fix ready for implementation into production. If a patch is not ready by the 96th hour, an estimate will be provided to the customer.
Severity Level 3 – Application is usable but requires a fix to correct a minor error.	< 4 days	Severity Level 3 problem shall be evaluated and, if required, scheduled for completion.

Figure 1: Table 2

a. The ASIS service-level standard can be impacted by a disruption in AWS and Subversion. If this type of disruption does occur, the ASIS System Network Manager shall be notified immediately, and he/she will execute the Information System Contingency Plan. ASIS customers are notified of service disruptions via a broadcast email.

6.7 Alternate Communications

a. *Between ASIS Team Members*

The ASIS Team uses a variety of redundant tools to support internal communication. These tools include Slack and Podio. The ASIS Team maintains, in Alfresco, the Aviation Safety Contact List, which includes postal addresses, email addresses, and phone numbers. In the event that one of these tools has a disruption in service, other tools can be used during the interruption. In the case of an interruption, the ASIS System Network Manager shall be notified immediately, and he/she will notify the ASIS Team and indicate what tool should be used to support internal communication. Once the issues have been resolved (by a third party), the ASIS System Network Manager shall notify the ASIS Team that normal communication between team members has been resolved.

a. *Between Customers and ASIS Team Members*

The ASIS Team has multiple redundant tools to communicate with customers. Our primary tool is Zendesk. However, the team can use email, telephone, and Mail Chimp as an alternative in the case of an interruption. Redundant contact information for customers is accessible in Zendesk, Podio, and Mail Chimp. In the case of an interruption, the WBAT Program Manager shall be notified immediately, and he/she will notify the customers/ASIS Team and indicate what tool should be used to support customer/ASIS Team communication. Once the issues have been resolved (by a third party), the WBAT Program Manager shall notify all customers/ASIS Team that normal communication between customers/ASIS Team has been resolved.

6.8 Order of Succession and Delegations of Authority

a. The ASIS Team maintains, in Alfresco, *Aviation Safety Org-Corporate*, an organizational chart that includes all employees, their supervisor, and, if applicable, who they may supervise. In the event that an employee becomes unavailable, their roles and responsibilities shall be delegated to their supervisor. In the event that the Vice President becomes unavailable, his/her roles and responsibilities shall be delegated to UTRS's Chief Operating Officer.

b. The *Aviation Safety Team Contact List* is maintained in Alfresco.