# DRAAS SERVICE GUIDE - DRAAS RESTORE TO CLOUD

Last Modification Date: 03/24/2023
Exported and Shared on: 03/19/2024

*For additional information, visit www.intervision.com*

# CONTENTS

# 1 OVERVIEW

DRaaS Restore™ proves your ability to recover offsite backups into the cloud or to the original site. This solution extends your existing Veeam investment by adding a cloud recovery option. The DRaaS Restore service also monitors and nurtures critical replication and recovery health components, providing insightful notifications to you and your InterVision service team to ensure recoverability is maintained.

## 1.1 COMMON USE CASES

- A low-cost recovery alternative, perfect for important applications that lack the urgency of faster recovery time solutions
- A reliable Veeam Cloud Connect solution with guaranteed cloud recovery resources and support

# 2 SERVICE DESCRIPTION AND DETAILS

- InterVision will provide the following:
  - DRaaS Restore to Cloud Account
  - Veeam replication target with Cloud Storage
  - The storage and computing capacity to power on your protected workloads
- Professional services are available to help determine the workloads you need to have protected, assist with the creation of a playbook and test plans, and assist during tests and declarations as part of the implementation fee or through paid consultation
- Internet, VPN or direct connect network can be used for replication
- Clients leverage their existing Veeam console to enable replication to cloud DRaaS repository
- Clients will continue to use their Veeam console for monitoring daily backups, routine restorations and managing the off-site data and retention policy. This can be managed as a BaaS Solution
- Restores from the cloud to the client's site can be performed by the client, per their standard operation of Veeam via their local console
- Recovery of a VM into a DRaaS Restore VPC will be performed upon request by the InterVision Support Team
- Cloud Usage and billing will be passed through the client invoice.
- Testing and Declaration:
  - Additional InterVision services beyond initiating the test workflow will be billed on a time and material basis.
- Recovery incidents are billed at an agreed-upon rate to restore the virtual machines. Time is billed only for restoration labor, not file copy wait times.
- Client site backup software, licensing, and management are available from InterVision for an additional fee. InterVision requires access to the number of backed-up VMs at the client site if renting a license from InterVision.

## 2.1 TEST AND RECOVERY SCENARIOS

The table below summarizes InterVision test and recovery scenarios and applicable fees. Fees will be clearly described in the customer's playbook.

| | Sandbox Test | Full Failover Test | Recovery |
|---|---|---|---|
| Declaration Fee | No | No | No |
| IaaS Resource Fee | No (up to 3 days) | No (up to 3 days) | Yes |
| Professional Service Fee | No* | No* | No* |
| Support Fee | No** | No** | No** |

* Typically, there are no Professional Services fees for a Test, but exceptions could be noted in the runbook by mutual agreement of actions, not in the scope of the managed service. This could include but is not limited to 3rd party device support, or additional planning and testing failback after a disaster declaration.

** Tests scheduled during standard Professional Support hours do not incur a support fee. If the client requests a test outside of standard Professional Support hours, "per incident" fees may apply. These are agreed upon at test scheduling.

Any work performed outside of the service guide and the details of the recovery playbook may incur professional services Costs.

# 3 REQUIRED SERVICES

- All Cloud DRaaS Restore environments require a minimum of AWS Business Support or Azure Standard Support

**Replication Targets**

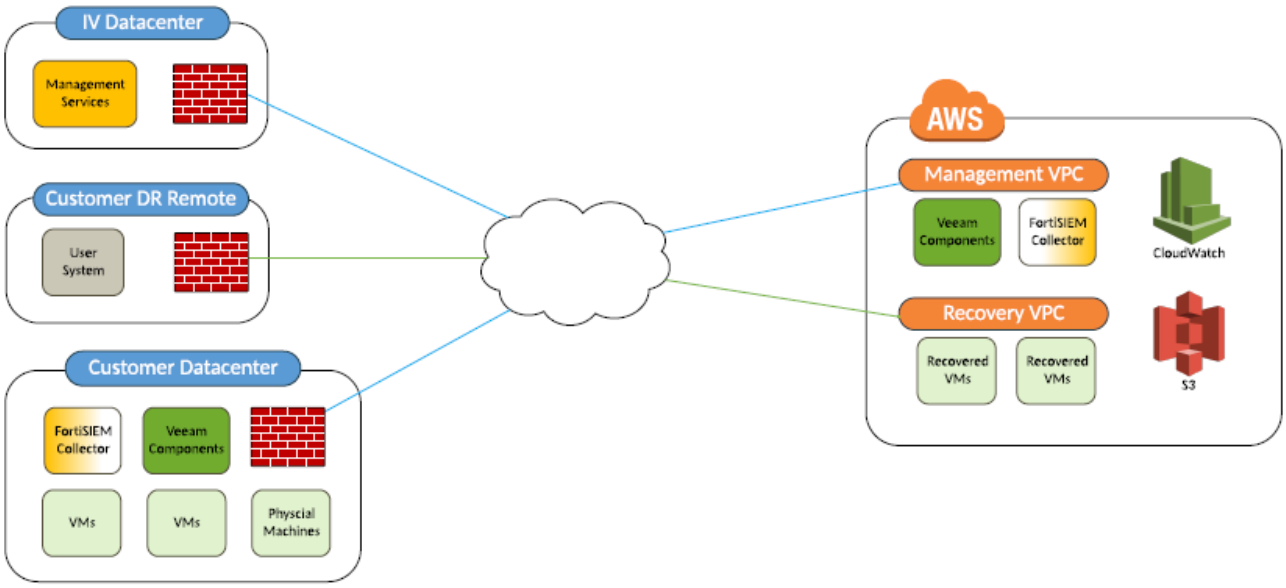
InterVision will create and manage the recovery environment that includes the resources (i.e. storage and compute) to build the virtual targets as well as the necessary cloud appliances to successfully replicate to the cloud.

The customer is responsible for all charges from Cloud Provider for the "DRaaS Ready Cloud Landing Zone". These charges are passed through to the customer on their InterVision invoice. Pricing indicated on the Service Order establishes a minimum monthly commitment. As changes occur and services are added additional fees may be incurred in the Cloud account and those charges will be passed through to the customer.

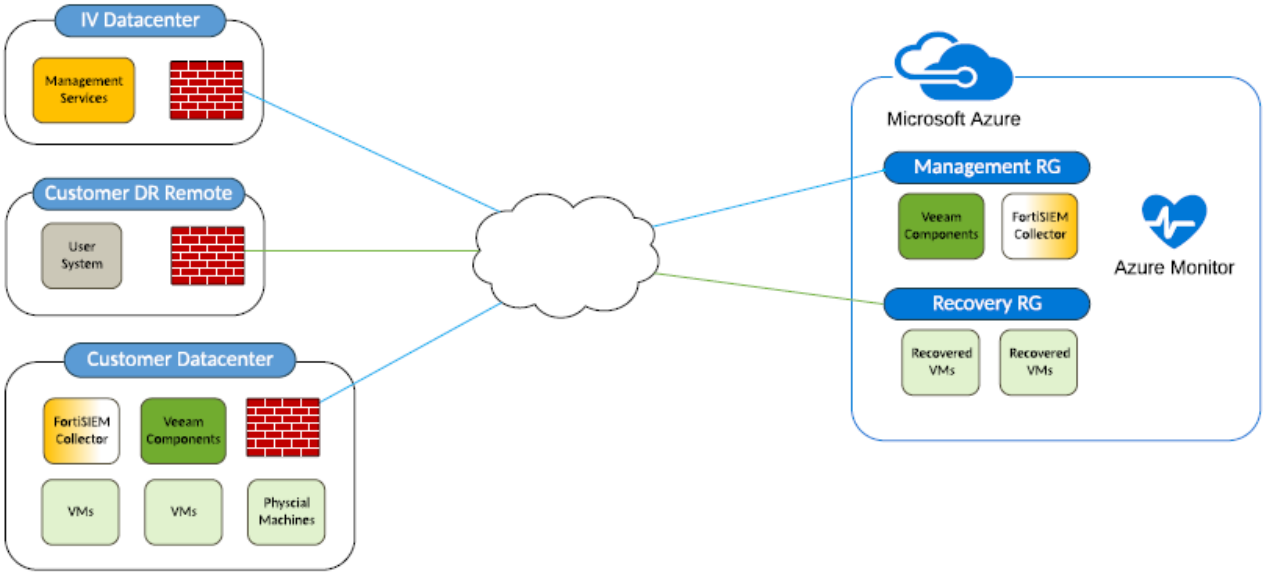
Changes that incur extra charges may include but are not limited to:

- Adding VMs to replication
- Adding storage to replicated workloads
- Running workloads in the DRaaS Ready VDC
- Declaring a disaster
- Running a DR test
- Reverse Replication
- Support plans

## 3.1 ARCHITECTURE DIAGRAMS



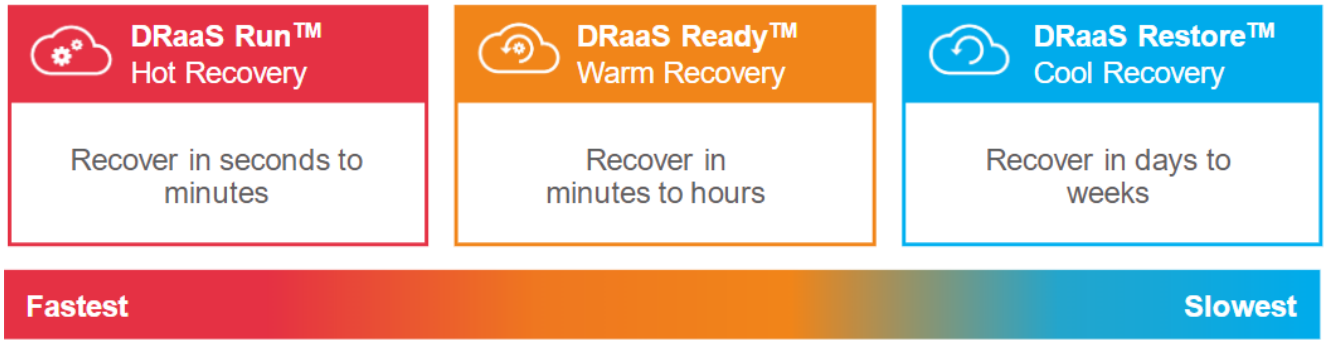

NOTE: Only one FortiSIEM Collector is required. Location is dependent upon use case.




NOTE: Only one FortiSIEM Collector is required. Location is dependent upon use case.

# 4 DRAAS OVERVIEW

InterVision DRaaS solution suite proves your ability to recover mission-critical services at desired time intervals, from seconds to days, that maximizes efficiency and cost-effectiveness. InterVision's world-class support and implementation teams will work with the customer to determine what recovery tier works best for each specific application/server. This managed service monitors and nurtures critical replication and recovery health components, providing insightful notifications to you and the InterVision service team to ensure recoverability is maintained.




DRaaS Run™ proves your ability to recover your mission-critical services in near real-time. It combines InterVision's enterprise-quality hosting infrastructure as an always-on virtual datacenter that runs a passive replica of critical services in a managed cloud environment.

DRaaS Ready™ proves your ability to recover your high-impact services within minutes to hours of a declaration. It protects the entire application, both physical and virtual machines, in one recovery environment.

DRaaS Restore™ proves your ability to recover offsite backups into the cloud or to the original site.

Portfolio shows real-time and historic evidence of recoverability and certified test results to provide you with confidence and proof you can share with your stakeholders.

# 5 SERVICE DESCRIPTION:

The DRaaS solution suite offers the following features and options to optimize your disaster recovery environment:

- Configuration documentation along with best practices on how to most effectively manage your services at InterVision
- Enterprise-class replication technologies
- Setup, support, monitoring, and management of the target cloud environment
- Replication traffic through the Internet, VPN or private network
- Storage and computing capacity to power on your protected workloads within the specified RTO
- Data encryption in-flight and at-rest
- Scheduled maintenance of the infrastructure performed during standard maintenance windows
- Testing and Declaration:
  - Compute resources are included in the base service cost for two annual, pre-scheduled test certifications initialized during standard support hours
  - Free test certifications must be scheduled at least 30 days in advance
  - Test initiation or support requested outside standard support hours will incur per-incident fees
  - Additional services beyond initiating the test workflow will be billed on a time and material basis. Fees will be indicated in the runbook if applicable.

- Upon test or declaration in Run and Ready environments, recovered VMs will be available for management and access through the VMware vCloud® Director™ interface in your Virtual Datacenter
- In Restore environments, recovery incidents are billed at an agreed-upon rate to restore the virtual machines. Time is billed only for restoration labor, not file copy wait times.
- Declarations will be treated as Priority 1 events

- Professional services can provide the following support:

- Determining workloads you need to have protected
- Determining appropriate RPO targets1
- Initial data seeding of recovery environments
- Assist with the creation of a playbook and test plans
- Assist during tests and declarations as part of the implementation fee or through a paid consultation

- Restores to client site via self-service or into InterVision cloud environment via Customer Support
- Client Portal to view replication jobs, policies, health information, and self-service capabilities

Because you are in control of your data center, virtual machines, and their replication, InterVision cannot guarantee an RPO for your specific workload.

# 6 SERVICE DETAILS

The InterVision Disaster Recovery as a Service (DRaaS) delivers the replication of virtual machines to an InterVision disaster recovery environment or to the public cloud.

Managed Virtual Machine Replication and Orchestration - InterVision utilizes 3rd party software to replicate, administer, and orchestrate the virtual machines and is available through the end-user web portal.

Monitoring and Support – InterVision will monitor the replication Service to ensure that the Service is running, remediate any issue related to InterVision-provided infrastructure, and provide reporting on any customer-impacting incidents. Monitoring information will be available to the customer via the client portal.

Service Runbook - InterVision will provide a DRaaS Service runbook template and assist with populating the runbook with information specific to the InterVision DRaaS Service.

Disaster Recovery Service Validation – InterVision will provide a DRaaS Audit and Testing that provides the ability to validate replication and failover services. The validation Service includes reviews of customer-specific documentation and runbook and target recovery resource pool and site-to-site connectivity. VM failover services will be tested. InterVision will provide a report of the failover readiness and consult of potential issues and recommendations. This Service is an additional fee and is required to maintain the service SLO promises to ensure the SLO can be met.

Recovery Services - InterVision will assist with virtual data center site failover upon request by the customer. The interVision service team will initiate the virtual machine failover operations, monitor the failover activity, and validate the virtual machines have been successfully failed over and are accessible. Tasks outside of the virtual machine replication and failover are outside of the scope of this Service and can be provided under separate work order. Application validation will be the responsibility of the customer.

Service Portals – InterVision will provide access to service portal for the following: service monitoring, VM administration, and for service request.

Scheduled maintenance - Infrastructure and Software maintenance will be performed and communicated in standard maintenance windows.

Initial data seeding services - are available for an additional fee. Contact InterVison's Professional Services for details and pricing information.

## 6.1 ROLES & RESPONSIBILITY MATRIX

| | Client | InterVision | Extended Services* |
|---|---|---|---|
| **General** | | | |
| Server and Application information (account, password, location, etc.) | X | | |
| Client escalation information | X | | |
| **Installation and Configuration** | | | |
| Determine the data to be protected | X | | X |
| Determine RPOs and RTOs for each application | X | | X |
| Provide the restore information including System details, folder path and/or file, file overwrite, etc. | X | | |
| Target system configuration | X | X | |
| Install replication software | X | | X |
| Create Replication Jobs | X | X | |
| Virtual target installation | X | | |
| Physical IaaS target installation (excluding O/S) | | X | |
| Physical non-standard target installation | | X | X |
| Replication license | | X | |

| | Client | InterVision | Extended Services* |
|---|---|---|---|
| **Monitoring** | | | |
| Monitoring of DRaaS Ready replication jobs | | X | |
| Monitoring of DRaaS Restore replication jobs | | | X |
| Monitoring of non-standard targets | | | X |
| **Incident and Problem Management** | | | |
| Software and configuration support | | X | |
| Event Notification | | X | |
| Replication job issues | | X | |
| Failover and recovery of protected systems** | | X | |
| Failback planning and migration Post DR declaration | | | X |
| Malware and Ransomware removal | X | | |
| Maintenance and updates replication software | | X | |
| Virtual target | X | | X |
| Physical IaaS target and infrastructure (firmware) | | X | |
| Physical non-standard target and infrastructure (firmware, O/S, etc.) | X | | X |
| Administer SW feature releases and non-critical updates | | X | |

| | Client | InterVision | Extended Services* |
|---|---|---|---|
| **Management** | | | |
| Provide customer requirements (maintenance windows, reboot schedules, etc.) | X | | |
| Administer user access to portal | X | X | |
| Customer change management and notification | X | | |
| InterVision notification of replication infrastructure maintenance events | | X | |
| **Reporting** | | | |
| DR Playbook | | X | |
| Custom Recovery Reports | | | X |
| **Replication Policy Management – Post Implementation** | | | |
| Replication redesign | | | X |
| Disaster Recovery Playbook Updates | | X | |

* Extended Services are services that may be provided at a cost incremental to the monthly recurring fees.

**May require additional professional services fees for a disaster declaration. or testing outside of standard support hours.

# 7 SERVICE ACTIVATION

All implementations are treated as a project and owned by the InterVision Project Management Office. The Project Manager, Implementation Consultant, and a Cloud Resiliency Team(CRT) member are the primary points of contact during the deployment of a DRaaS solution. Common step to service activation:

1. Project kickoff call with the client to introduce the project team, understand requirements/key dates for the project.
2. Technical data gathering from the client
3. Deployment of the client environment in the replication target
4. Review with the client how to connect to their environment

# 8 COLLABORATIVE IMPLEMENTATION

1. Install appropriate replication technology in the client's production environment
2. Connecting client production environment to target (typically a VPN or dedicated PtoP)
3. Initiate replication of client Virtual Machines
4. Configuration of recovery firewall to match production configuration.
5. Upon completion of replication, a test plan is drafted for an initial DR test
6. The client performs test of DRaaS environment with our assistance
7. Review findings with the client
8. Draft Playbook based on test plan and test findings
9. The playbook is revised until mutually agreeable.
10. Schedule Portfolio training with the client
11. Transition to steady-state operations with Cloud Resiliency Team

InterVision recommends repeating steps 6-11 twice annually with the assistance of the InterVision Customer Support Team.

# 9 SERVICE ITEMS

The following service items may be included when purchasing the DRaaS Solution suite.

| |
|---|
| IaaS Resources |
| • CPU<br>• Memory |
| Licensing |
| • DRaaS Replication License (Zerto)<br>• DRaaS Restore Cloud Connect License (Veeam)<br>• DRaaS Backup License (Veeam) |
| Storage |
| • Standard, Encrypted<br>• Ready<br>• Archive |
| Replication Traffic |
| • 1GB Port<br>• 10GB Port<br>• Internet<br>• In-Cloud Replication (Data Flow)<br>• IP Address |

| At Recovery |
| --- |
| • CPU at Recovery<br>• Memory at Recovery<br>• Storage - Standard at Recovery<br>• Max Bandwidth at Rec - 10 Mb<br>• Max Bandwidth at Rec - 100 Mb<br>• Max Bandwidth at Rec - 1 Gb |
| DraaS Service Management |
| • Replication Service - Ready Virtual<br>• Replication Service - Restore Service |

# 10 DEFINITIONS

**Landing Zone:** is a predefined operating environment designed and built for the purposes of supporting the InterVision service, providing the compute and network resources for recovery.

**Client Content:** Electronic data or information submitted by Client to the Disaster Recovery Service

**Declaration:** The announcement by preauthorized personnel that a disaster or severe outage has occurred (or is imminent) that triggers predefined response actions.

**Declaration Event:** is the Client has notified InterVision in writing (such as a support ticket) of intent to use the DRaaS VDC as the primary environment, i.e. to recover and resume production in the DRaaS VDC. Declaration Events are verified according to InterVision protocols.

**DRaaS Runbook (Playbook):** is a predefined staged task list to achieve recovery for disaster events. To be developed during disaster recovery testing.

**DRaaS Virtual Data Center:** and **DRaaS VDC:** shall mean an environment provided to Client by InterVision for purposes of replicating data and for recovering the virtual machines and data upon a Declaration Event. These are Run, Ready and Restore VDC types.

**Failback:** the process of re-synchronizing that data back to the primary location, halting I/O and application activity once again and cutting back over to the original location.

**Failover:** the process of shifting I/O and its processes from a primary location to a secondary disaster recovery (DR) location. This typically involves using a vendor's tool or a third-party tool of some type that can temporarily halt I/O, and restart it from a remote location.

**Full Failover Test:** An actual failover of the protected workload to the target site. Failback is needed to return the workload and any updates or transactions to its primary datacenter. A successful Sandbox Test is highly recommended before performing a Full Failover Test to reduce the risk of potential application disruption.

**Journal**: Contains the recovery checkpoints for the environment, stores continuous checkpoints for failover based on RPO and Retention settings.

**Recovery Point Objective (RPO):** point in time in which data must be recovered to avoid unacceptable data loss in a disaster situation.

**Recovery Time Objective (RTO):** is the target time for the recovery of your Virtual Machine after a disaster has struck. InterVision will validate the virtual machine boots and operates. Client testing and validation that the application is operational is beyond the InterVision RTO.

**Replication:** is the Managed Service activity that manages and transfers the Client's data to the DRaaS VDC in a Replication State.

**Replication Service:** is the Managed Service pertaining to the replication activities and is a function of the number of Client Virtual Machines being replicated, or the amount of Storage consumed.

**Recovery:** The process of promoting a protected workload into full operation.

**Recovery Test:** is a test of the recovery processes and the DRaaS VDC environment in Recovery State that stops short of making it the primary production VDC for any period.

**Recovery State:** is the period between a Declaration Event and the time the Client has resumed production in the original primary environment or has converted the DRaaS VDC to a production VDC.

**Sandbox Test:** Allows for testing a copy of the protected workload in isolation at the target site with all updates or transactions being discarded upon completion.

**Virtual Protection Group**: A prioritized collection of Virtual Machines that must be recovered together

**Zerto Cloud Appliance**: Manages the three Zerto services within Amazon Web Services EC2 instance. The three services included in the Zerto Cloud Appliance:

- **Zerto Virtual Manager:** Manages disaster recovery, business continuity and offsite backup functionality at the site level
- **Zerto Virtual Replication Appliance**: Replicates the VMs and virtual disks
- **Zerto Backup Appliance**: Manages offsite backup operations. Runs as a service at the target site, in this case, in Amazon Web Services and enables the backup of replicated data. There is no host in ZCA.

# 11 DISASTER RECOVERY AS A SERVICE LEVEL OBJECTIVE AND COMMITMENTS

**DRaaS Availability**

Availability SLA's are provided in the Managed Services Statement of Work (MS-SOW)

## 11.1 RECOVERY SERVICE LEVEL COMMITMENTS

**Recovery Point Objective** (RPO): The RPO will be determined by the Service Offering and the underlying technology architected to provide the solution. InterVision will perform the best effort to keep the RPO within the time specified in the customer's Playbook. The customer will be alerted should the solution fall out of the RPO set.

**Recovery Time Objective** (RTO): The RTO will be determined by the Service Offering and the underlying technology architected to provide the solution. The RTO SLO only applies to the Managed Service experiences. The RTO will be specified in the customer's Playbook developed during implementation.

The term **"Disaster Recovery Declaration"** is defined as follows:

A substantial outage of the Client's IT infrastructure in which the Customer declares a disaster event. This Customer declaration activates the process of executing the Customer Disaster Recovery Plan documented in the InterVision DRaaS Runbook (Playbook). This DRaaS Runbook includes steps to transition primary Customer IT operations from the Primary location to the designated Disaster Recovery location.

InterVision will require a customer representative with a defined role of "Recovery" in the InterVision Portfolio Admin Tool to initiate the disaster declaration prior to creating a P1 ticket (emergency) for the event. Subsequent steps will be dictated by the Customer and in accordance with the Disaster Recovery Plan.

**DRaaS Service Credits for Declaration State**

When a client invokes a Disaster Recovery Declaration Event for a DRaaS VDC into a vCloud environment, (i.e. Run, Ready, and Restore); the IaaS Premium Service Level Objectives and Service Level Commitments apply and all resources within the contracted capacity specified in the Sales Order will be available and all Virtual Machines that can recover within the contracted capacity will be powered on unless otherwise specified.

Exclusions

The following are not covered by this SLO:

- The customer is solely responsible for generating and formatting all data.
- The customer is solely responsible for the integrity of all data targeted for DRaaS.
- Failure of the customer's Internet or other network connection to the DRaaS servers (e.g. via the public Internet or the customer's network).
- Malfunction of customer's computing systems upon which the DRaaS components are installed (including hardware, operating system(s), or local software) – including lack of availability due to configuration issues.
- Inability to access DRaaS due to customer security or software provided by customer or 3rd
- For DRaaS products that target AWS for their recovery: InterVision will initiate all actions defined in the Recovery Run Book. Services beyond the scope of the Run Book, including steady-state operations after the declaration, will require a separate statement of work and may incur additional professional service costs.