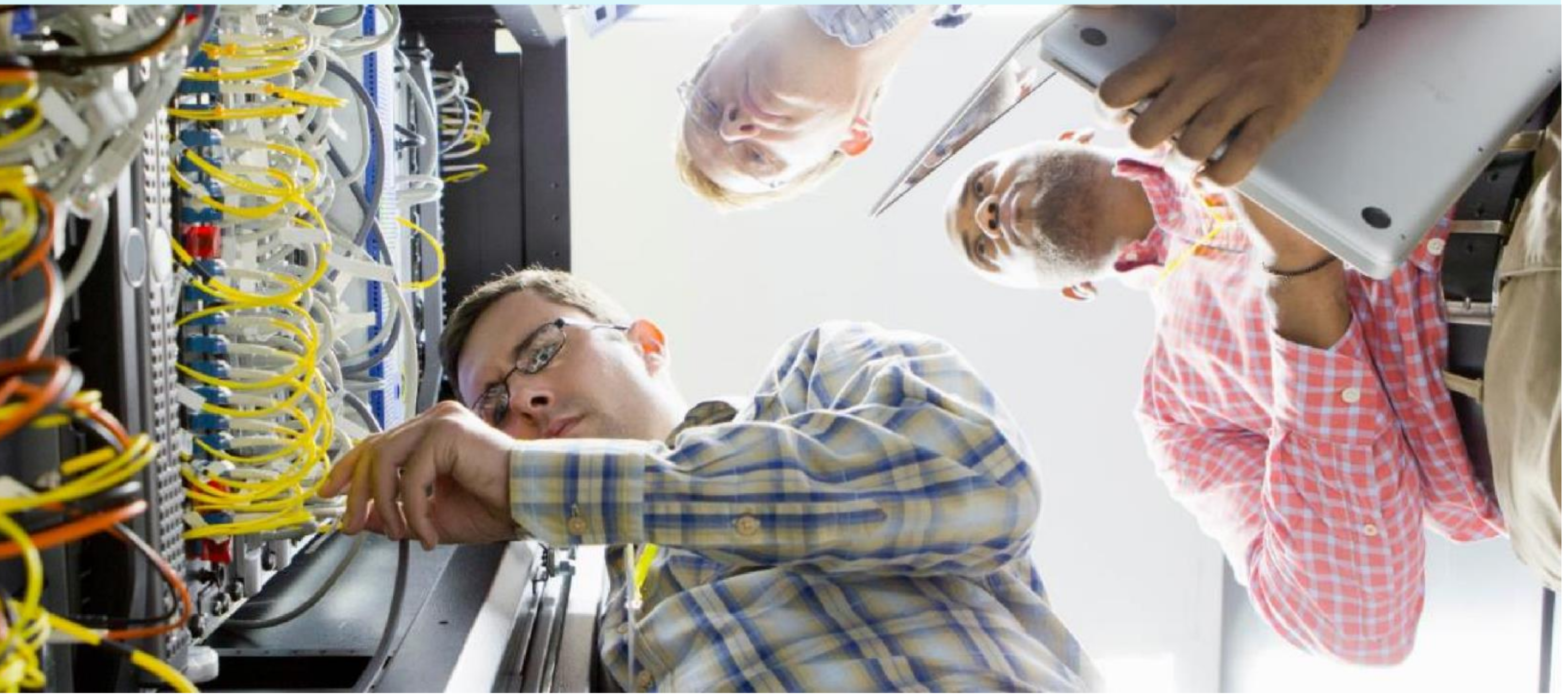
Optum

Enterprise Disaster Recovery Program Overview

August 2023



Contents

Section I – Enterprise Disaster Recovery Overview

Background

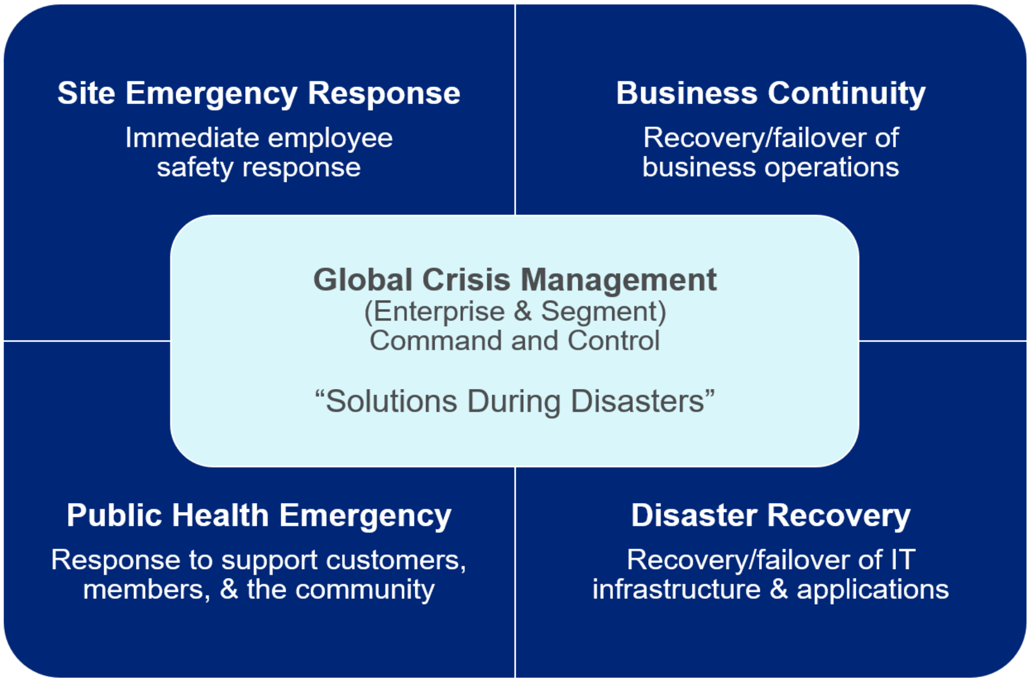
The purpose of this document is to provide an overview of the Enterprise Disaster Recovery (EDR) Program managed within Optum Technology supporting the entire UnitedHealth Group Enterprise.

UnitedHealth Group relies on a diverse array of interconnected information systems to meet the needs of its clients. The goal of disaster recovery (DR) planning is to protect the organization in the event that all or key aspects of UnitedHealth Group operations are rendered unusable due to an unforeseen disaster event affecting the corporation’s IT systems. Preparedness is the key. The company has instituted an Enterprise Disaster Recovery Program (the Program) to first eliminate or reduce disaster risk in critical technology areas, and then plan for facilitation and the timely and predictable restoration of key applications, data, and supporting critical infrastructure.

The Layered Program Model

UnitedHealth Group understands the importance of contingency planning. Protecting the assets of the corporation is a high priority. The layered Program model focuses on ensuring consistency between the organization’s crisis management, site emergency response, corporate security, business continuity, disaster recovery and public health emergency planning efforts. These layers are interrelated and work together to provide maximum protection and risk mitigation.

The model contains the following key components:



Site Emergency Response
Immediate employee safety response

Business Continuity
Recovery/failover of business operations

Global Crisis Management
(Enterprise & Segment)
Command and Control

“Solutions During Disasters”

Public Health Emergency
Response to support customers, members, & the community

Disaster Recovery
Recovery/failover of IT infrastructure & applications

The EDR Program functions in conjunction with the Business Continuity program as part of UnitedHealth Group’s Enterprise Resilience. The Program focuses on the loss of critical technology, systems, and applications. During any given year, there are many UnitedHealth Group Business Continuity events but very few of these events become a Technology Event and the actual declaration of a technology disaster is not a common occurrence.

Mission and Objectives

The mission of the Program is to minimize the aggregate risk and impact to UnitedHealth Group from the occurrence of disaster events, focused on the overall viability of UnitedHealth Group to survive an event.

The objectives of the Program that are in support of the mission are:

- Provide a “systems solution” that accommodates the interdependencies between business processes and applications.
- Drive systemic improvements in DR capability (e.g., Recovery Time Objective (RTO), etc.).
- Recognizing funding and time constraints, evolve and improve the DR capability in a manner that provides greatest good for greatest number.
- Provide DR requirements as part of UnitedHealth Group’s systems architecture, delivery and operations as opposed to an after-thought once a new application goes into production.
- Develop and deploy a modular, adaptive set of capabilities rather than one size fits all.
- Deal with the most probable DR scenarios in addition to worst case “smoking hole”.
- In addition to protecting UnitedHealth Group’s on-going viability, make the DR capability a competitive strength in the market.

Policy

The company recognizes and acknowledges that the protection of its assets and business operations is a major responsibility to its employees, shareholders, business associations, customers, and other communities that it services. Therefore, it is Optum’s policy that business continuity and IT disaster recovery plans must be developed, tested, and maintained to limit losses caused by disruptions to critical business operations and to enable efficient and effective recovery. The Program includes processes and controls to protect the business of Optum, the life and safety of workforce members, as well as to protect the image, reputation, assets, and resources of the organization.

By policy, DR plans must be developed and maintained for all core infrastructure and applications identified as business critical within the business continuity plans. DR Plans must be updated, exercised, and approved by appropriate leadership annually or biennially as mandated per corporate policy. The Program include processes and controls to protect the business of UnitedHealth Group, the life and safety of workforce members, as well as to protect the image, reputation, assets, and resources of the organization.

Optum Technology Overview

It is difficult to describe the EDR Program without an understanding and overview of the Optum Technology environment. The Program does not stand alone but is integrated into the Optum Technology computing processes and day-to-day operations.

Optum Technology’s mission is to help people live healthier lives and to help make the health system work better for everyone. Optum Technology is a comprehensive, large scale and international information technology organization, developing technology solutions to support the UnitedHealth Group mission and core businesses of care management, benefit administration, health financials and health analytics. Optum Technology is a Healthcare technology leader in providing computer processing services delivered through Optum Technology’s portfolio of services with world-class efficiency and effectiveness.

The majority of UnitedHealth Group’s enterprise infrastructure is not outsourced to a vendor, but is wholly owned and managed by Optum Technology. Optum Technology may also use public cloud offerings where appropriate.

Optum Technology is committed to delivering innovation and state-of-the-art technology that improves customer experiences, improves care, and provides superior early predictions. This involves a variety of different technology disciplines including:

- Software Engineering & Advanced Technology
- Data Management and Analytics
- Infrastructure and Cloud Services
- Security and Risk Management

With a focus on advanced and emerging technologies to accelerate consumer and clinical benefits while reducing operating costs:

- Artificial Intelligence & Machine Learning
- Blockchain
- Individual Health Record (IHR)
- Internet of Things (IoT)
- Natural Language Processing (NLP)

Optum Technology's health care technology experience and high-volume capacity offer secure, scalable, and seamless technology for our customers. Everyday Optum Technology technical teams support the following:

- 21,000+ global technology professionals responsible for computing hardware, software, and communications.
- Primary Tier 3 data centers in Minnesota with nearly 20 MW capacity
- 100,000+ servers, 7 IBM z-OS mainframes.
- Over 150 petabytes data stored in secure data centers.
- 326,000 voice/data ports with our Virtual Contact Center supporting +300 million calls annually.
- Supporting over 250,000+ users.
- Global development organization – primary locations in CA, MN, NJ, PA, CT, India, Ireland, Manila.
- 7000+ applications supporting the UnitedHealth Group businesses.
- Over 1 trillion computing transactions annually.
- More than 2.8B claims processed annually with more than 99.5 percent accuracy.
- 1B+ Web and mobile transactions annually.
- Providing Health and Information Services to 1 in 5 Americans.

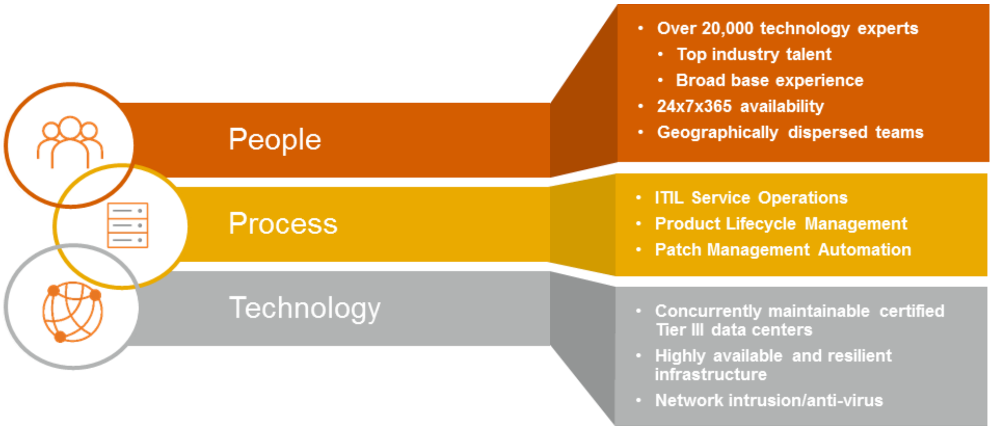
Disaster Recovery Strategy

Optum Technology's approach to DR is based on two fundamentals: Prevention and Protection. A focus on balancing the combination of disaster prevention and protection results in reducing both the probability and impact of a disaster. The goal is to first eliminate or reduce disaster risks in critical areas, and then plan for the most probable disaster scenarios.

Prevention

For many companies, disaster recovery means minimizing downtime as they try to restore systems and get them back online. Optum Technology's strategy includes focusing on items that would assist in preventing a disaster from taking down systems in the first place.

Optum Technology has invested in creating an effective combination of people, process and technology that provides the fundamentals for a proven production method resulting in a stable, scalable environment for our applications to perform at operational excellence. This investment creates the "prevention" which is fundamental to the Program. Prevention is the proactive remediation of known technology exposures and includes removing "accidents just waiting to happen".


People
Process
Technology
Over 20,000 technology experts
Top industry talent
Broad base experience
24x7x365 availability
Geographically dispersed teams
ITIL Service Operations
Product Lifecycle Management
Patch Management Automation
Concurrently maintainable certified Tier III data centers
Highly available and resilient infrastructure
Network intrusion/anti-virus

Optum Technology is a team of over 21,000 Information Technology professionals responsible for computing hardware, software, and communications. Over 5,000 of these individuals are technology infrastructure experts. Optum Technology recruits and develops many of the finest talents in our industry, as IT skills are central to our success. Optum Technology's is a global organization with primary locations in CA, MN, NJ, PA, CT, India, Ireland, and Manila. Technical staff works as virtual teams (also known as a geographically dispersed teams). Many of our technical teams are office based, but a percentage of them telecommute and work out of homes offices. This has allowed the organization to hire and retain the best people regardless of location. These geographically dispersed virtual teams strategically position Optum Technology technical staff to be able to provide business continuity in the case of any event no matter where the location.

Optum Technology has system operations and facilities management teams that work 7x24. The technical teams operate with on-call rotations providing access to technical staff at any time of the day or night. This is complemented with core offshore technical resources which have been trained and are available to assist in an event if needed. Having trained technical employees located around the world reduces the risk of an event occurring that would disable coverage from our technical workforce. The Optum Technology technical teams have business continuity plans that are exercised annually as business continuity planning is not an option; UnitedHealth Group understands that it is a necessity.

Optum Technology's data centers and technology are self-managed, and Optum Technology has instituted a formal IT Infrastructure Library (ITIL) based service delivery model.

Optum Technology leverages a number of technologies to reduce the probability of a disaster. These include the failover of production processing to geographically dispersed production or non-production systems; geographic load balancing; asynchronous data replication of production storage pools; software-based database asynchronous replication; and media data restores. These capabilities combine to help achieve the objective of resuming operation with limited to no data loss or disruption to stakeholders.

Core to the recovery solution design for Optum Technology is a multiple data center approach. The primary data centers for Optum are located in the Minneapolis/St. Paul metro area, which is not prone to large-scale disasters such as hurricanes. Optum Technology chose an ”in-region” strategy as the most effective approach to providing data center redundancy for our needs.

- An in-region strategy allows for a "system" of data centers to be deployed that are connected with very affordable and yet high capacity, high availability networking. Although history is not an absolute indicator of future events, historical research of climatic events contributed to the careful selection of sites to locate data center facilities to minimize the impact potential of a single event.
- The in-region "system" approach allows Optum Technology to place processing requirements in both cost-optimized and functionally optimized configurations. Tape processing (physical or virtual) is placed in a different data center than the on-line processing. This also allows for more robust disaster recovery capabilities (very low recovery time objective and recovery point objectives) provided at a fraction of the cost that would be incurred in an out-of-region or outsourced approach.

Optum Technology’s latest data centers were built to a Tier 3 level with all the necessary environmental redundancies including critical areas of the building and the outside plant able to withstand 200+ mph winds or the strongest F3 tornado.

The multi data center approach includes criteria for strategic placement of the critical application’s production processing as well as recovery, development, and tape management environments. Each of our key data centers includes an Operational Command Center with 7x24 staff actively monitoring the components and systems. If there was an event in one of the Optum Technology data centers, staff located at the other data center would continue system operations. Optum Technology has a dedicated data center facility management team that monitors, proactively maintains, and manages all aspects of these data centers. The offsite storage for tape is within an Optum Technology controlled data center facility located within the region that provides full environmental redundancies.

Optum Technology is committed to using state of the art technology. The EDR Program surpasses other Healthcare technology providers due to the following technology services Optum Technology has deployed:

- Providing excellent Customer Service remains a top priority for Optum. Receiving and resolving calls from clients is a large and critical part of our business. Optum Technology has implemented a Virtual Contact Center that dynamically routes a million calls daily across 40+ contact centers and 20,000 service agents. If there is an event at a remote call center, incoming calls can be immediately rerouted to alternate call centers for processing and resolution, reducing any impact to our clients.
- Storage virtualization compliments server virtualization in increasing the portability of host systems through consolidation and replication allowing them to fail to an alternate site quickly, reliably and in large numbers.
- A standard desktop is used by Optum staff across the enterprise. In case of an event, replacement laptops can be immediately dispersed to the staff, and because all staff use the common configuration, they can be productive and resume their business process functions quickly.

While Optum Technology’s focus is to prevent disasters, it also recognizes that there is always the potential for a disaster to occur and has developed strategies to protect the business should there be an unforeseen event.

Protection

Completely avoiding a technology disaster is impossible. However, the EDR Program is based on anticipating and planning for the common types of disasters and designing solutions to address them. Disaster protection addresses recovery from the most probable disaster scenarios and a worst case “smoking hole” scenario. The EDR strategy involves identifying critical business processes and transitioning these critical applications, data, and supporting infrastructure to an alternate recovery location in a timely manner, thereby reducing the impact of a technology event to our critical business clients.

The EDR Program utilizes a variety of recovery strategies which align to the defined criticality of the application. Business critical applications, as defined by the Business Impact Analysis (BIA) and subsequent Business Continuity Plan (BCP), are given the highest priority and generally have a 72 hour or less Recovery Time Objective (RTO).

The RTO is the period of time within which systems, applications or functions must be recovered after a disaster outage is declared. The RTO is measured in hours or days and is an important consideration in recovery planning. The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by the business. This is generally a definition of what an organization determines is an “acceptable loss” of data in a distressed situation. The RPO is expressed backward in time (that is, into the past) from the instant at which the failure occurs and can be specified in hours or days.

Highlights of the DR protection components include:

- Optum Technology data centers can operate in a “Lights out” mode for up to 3 days. If the Data Center continues to get fuel to run the generators, they are designed to run in this mode indefinitely.
- Operational backups are designed to use high performance disk-to-disk primary copy with physical offsite second copy to virtual tape libraries.
- Active-Active recovery designs which utilize two geographically separate data centers with global load balancing where both sites are fully supporting the production application. In the event of the loss of a single datacenter, the application continues to function with no intervention required.

- Active-Standby recovery designs which utilize two geographically separate with one site fully supporting the production application. In the event of the loss of the Active site datacenter, manual intervention is required before the application is returned to service.
- Native Database replication technologies can be utilized depending on the related database technology in either an Active-Standby or Active-Active methodology.
- Mainframe SAN Replication recovery utilizes full asynchronous data replication between the production mainframe and a geographically dispersed hot standby DR mainframe.
- Other storage replication technologies are utilized in specialized areas such as with VMware Site Recovery Manager (SRM) or IBM iSeries replication.
- Some distributed systems employ a Cold recovery solution with failover of production to geographically separate non-production systems utilizing data restoration from virtual tape.
- Each application identified as critical within corporate business continuity plans has a DR Plan that is refreshed at least once each year and tested annually.
- Metrics in the form of Key Risk Indicators (KRIs) are used to derive the “health” of application DR plans.

Optum utilizes a number of different architectures that provide flexibility in the delivery a DR solution.
Either applications can contain a single consistent DR solution, or they can contain multiple DR solutions. Where multiple DR Solutions are in use the overall application RTO is reported as the longest single component’s RTO. For example, an application that has Cold and Standby components would have an overall application RTO of 8 weeks.

Lifecycle Maintenance

Existing DR Plans follow standard lifecycle maintenance and are updated as changes occur to the applications or associated systems but must be refreshed at least annually. It is the responsibility of Application Owners and the Enterprise DR Team to ensure Plans are reviewed to identify:

- Equipment updates or changes.
- Contact changes (such as role changes or resignations).
- Changes in business requirements not reflected in specific plans.
- Changes in application that impact recovery or validation procedures.
- Inaccurate assumptions or oversights.

Application DR Plans are approved and certified annually or biennially by the appropriate Application Owner with the organization. Failure to complete a new DR Plan on time or complete an annual update of a DR Plan requires that a policy exception be submitted in Optum’s Enterprise Governance Risk Compliance system (EGRC) by the Application Owner.

Section II - Roles and Responsibilities

Enterprise Disaster Recovery Team Responsibilities

The Enterprise DR team facilitates, oversees, advises, manages, and tracks all aspects of the recovery as it progresses. The Enterprise DR team manages the following recovery planning tasks as required:

- DR Program compliance across the UnitedHealth Group enterprise.
- Coordination with the Enterprise Response and Resiliency Program.
- DR Program coordination with LOB DR Leads to comply with DR Policy.
- Facilitation DR Plan update processes and annual approval of DR Plans.
- Tracking annual DR exercises, findings, and remediation tracking of exercise issues.
- Subject Management Expert supporting responses to auditors and/or regulators regarding DR information, program, or exercise results.
- DR Program coordination with Optum Technology to continuously review overall DR capabilities to determine and guide potential improvements.
- Training related to recovery topics including tabletop and certain functional exercises.

- DR reporting through DR Key Risk Indicators (KRIs).

Enterprise Disaster Recovery Coordinator Responsibilities

Each Enterprise DR Coordinator (DRC) is assigned to assist Application Owners with the development, maintenance, exercising and implementation of application disaster recovery plans.

The DRC performs the following recovery planning tasks as required:

- Schedules and facilitates meetings with Application DR Coordinators to develop and/or maintain DR Plans for critical business applications. The Application DR Coordinator is typically the Service Level Owner (SLO).
- Reviews DR Plans for completeness and accuracy of content before plans are submitted for approval.
- Participates when needed in tabletop and functional DR exercises.
- Identifies appropriate technology resources and participates in DR requirements determination process and application vetting meetings.
- Supports the maintenance activities for draft and production DR Plan information.

Application DR Coordinator (SLO)

The SLO is the primary person within the Application or Infrastructure team that provides operational support for an application/infrastructure. The SLO performs the following recovery planning tasks as required:

- Owns their specific application/infrastructure DR Plan.
- Responsible for completing the development of new DR Plans and the annual refresh of existing DR Plans.
- The primary point of contact for the Enterprise DRC.
- Owns the recovery and validation process for their application/infrastructure at time of event.
- Identifies when an Alternate Application DRC is required to support the completion of SLO responsibilities.

Line of Business Disaster Recovery Lead Responsibilities

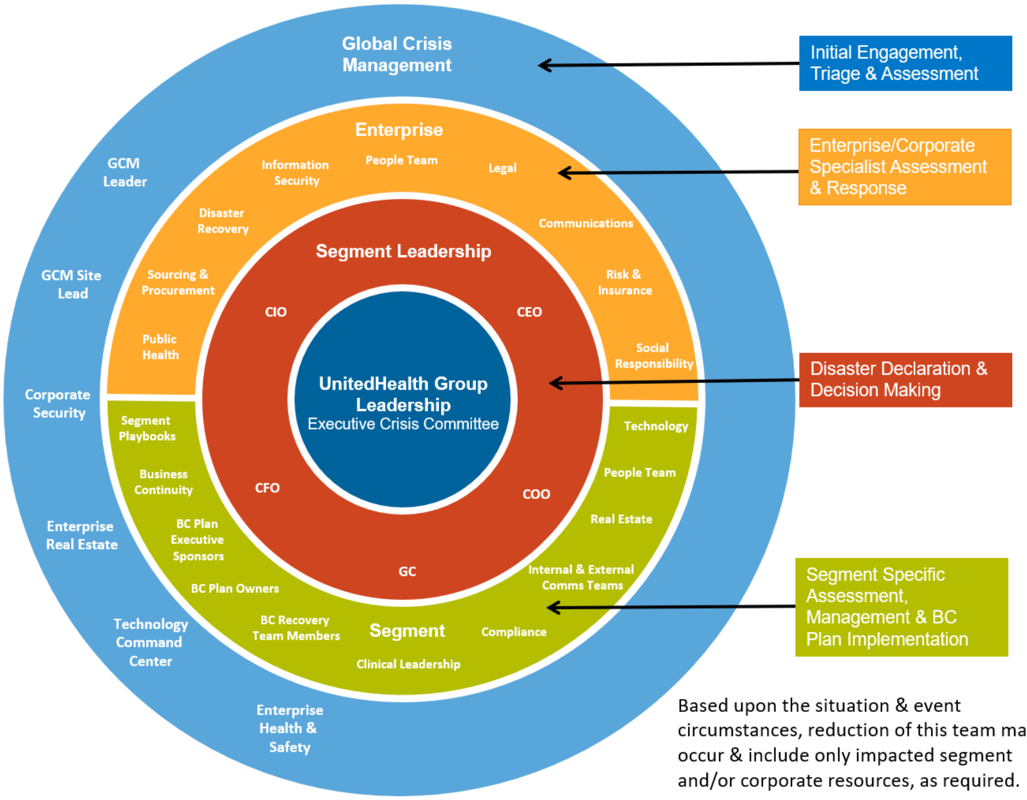
The DR Lead is designated by the business segment or application group to head the disaster recovery effort for specific applications by managing and directing the following disaster recovery tasks as required:

- Ongoing validation of critical applications to ensure:
  - Critical business processes are identified and correct.
  - Business process criticality scores accurately reflect criticality of the application.
- Review and drive resolution of application risks related to DR (e.g., unacceptable DR solutions).
- Drive strategic improvement and investments related to DR.
- Provide oversight of DR plans for completion, approval, and accuracy.
  - Application/infrastructure changes are reflected in the DR plan on a timely basis.
- Provide oversight of functional exercises to ensure:
  - Functionally exercisable application components are exercised annually and as change occurs.
  - Results are reported in a timely fashion.
  - Exclusions from the functional exercise requirement are reviewed, challenged as necessary and approved if valid.
  - SLO's are aware of the proper exercise process and purpose.
- Ensure that DR is always considered when changes are made that could impact recovery.
- Identify contractual and regulatory requirements relating to DR for applications.
- Support external customer responses and requests relating to DR (e.g., audits, contracts, RFPs)
- Participate in EDR DR Lead Program. Attend workshops, round-tables, office hours, etc.

Global Crisis Management Team Responsibilities

The primary purpose of the Global Crisis Management team is to prepare and respond to crisis impacting UnitedHealth Group. The Program ensures continuity of care & pharmacy, protection of employees, operations, assets, data, and reputation. Subject matter experts, both at the corporate and segment level, continue to manage actions within their functional teams, however, will leverage the crisis management team as a forum to engage, communicate and make decisions between teams more quickly and reliably. The crisis management team will:

- Coordinate all-hazards response system to facilitate quick decision making and communications between executives and operational teams around the globe.
- Maintain trained and exercised Crisis Management Teams of subject matter experts across the business that can be engaged and respond quickly to crisis.
- Provide proactive situational awareness of risk/hazards that may impact business operations.
- Build a culture of readiness and preparedness.
- Engage the following functional leaders or appropriate alternatives, as required:



Based upon the situation & event circumstances, reduction of this team may occur & include only impacted segment and/or corporate resources, as required.

Section III - BC and DR Prioritization

Business continuity planning requirements are driven by a business impact analysis (BIA), supporting the company's Enterprise Risk Management discipline as an integral part of UnitedHealth Group's culture, decision-making processes, and governance processes. The BIA, combined with threat and risk assessments, helps assure that business continuity risks are appropriately prioritized and remediated by applying cost effective strategies and mechanisms to reduce risk to a tolerable level. The enterprise business impact analysis process:

- Identifies potential impact of uncontrolled, nonspecific events on UnitedHealth Group business processes and its customers.

- Considers all business segment functions; and
- Provides an estimation of maximum allowable downtime and acceptable levels of data and operational loss.

Each critical function is required to perform a risk assessment utilizing the business impact analysis, threat and vulnerability assessment, and gap analysis of business continuity mechanisms currently in place. The result of this risk assessment is a segment commitment to reduce risk to an acceptable level within reasonable resource and budgetary constraints.

Within the BIA, an analysis is done to determine the level of criticality of a process and establish a Process Criticality Score. As the Segment Business Continuity Leads (BCL) work with the business to create Business Continuity Plans, they work with the business owners to determine which applications are required to support each business process.

Applications supporting the critical business processes identified are given the process criticality score. The DR tier is assigned to the application based on the process criticality score. Tier 0 is reserved for critical infrastructure applications.

UnitedHealth Group recognizes that planning for disaster recovery is essential to mitigating risk to the business. Building a DR solution for an application that is associated with a critical business process (as deemed through the UnitedHealth Group Business Continuity Program as described above) is required. This includes designing and implementing the appropriate DR infrastructure capability, as well as creating the supporting recovery documentation (DR Plan, critical contact lists, application recovery scripts, and validation procedures), and eventual exercising of the DR solution.

Application Vetting Review

The Business Continuity team provides potential new critical DR applications to the Enterprise DR team as applications are identified or changes occur. The Enterprise DR Team works with the Business Continuity team along with the BC plan owner and application owner to determine the appropriate tier status for the identified application. Once an application is identified as DR critical, the Enterprise DR Analyst begins the development of DR Plan. This work is completed with the support of the Segment DR Lead and Application DR Coordinator to determine and document in the DR Plans:

- Location of production and non-production sites
- Size of production and non-production environments
- Type of production and non-production environments
- DR Capability and Solution

Disaster Recovery Plan Development

The Disaster Recovery plans are part of the overall EDR program designed and structured to respond to technology disaster events affecting our data centers, restore critical infrastructure and business applications, and resume normal business function operations in a prioritized manner. The DR plans focus on each of the identified critical business applications or infrastructure. The goal is to plan for the worst-case scenarios, such as the complete loss of a data center, so that we can react quickly and efficiently. These worst-case scenarios cover impacts from all types of events, both natural and manmade.

Disaster Recovery Plans

All application owners are responsible for the development and maintenance of a DR Plan for each critical business application or critical infrastructure to meet the needs of critical business processes and functions in the event of a disaster. The procedures for execution of such a capability are documented in a formal DR Plan, which is reviewed at a minimum on an annual basis and updated as necessary by the Application DR Coordinator in conjunction with the Disaster Recovery Lead and the Enterprise DR Coordinator. DR Plans are developed for critical business applications using standard tools and templates.

The Application DR Plans need to be maintained to sustain the organization's ability to be prepared for, respond to, manage, and recover from disasters affecting its mission.

The objectives of the DR Plan include, but are not restricted to:

- Reducing the critical impact that a catastrophic disruptive occurrence can have on UnitedHealth Group's critical business applications, cash flow and customers.
- Enabling the transition of critical application functions to an alternate recovery facility.
- Ensuring recovery of critical services to the affected business units and providing critical services to customers during a survival-mode stabilization period.
- Providing for time-phased restoration of critical business application processes and services after a disruption.

Plan Assumptions

DR Plans are based upon the following assumptions:

- The event which prompted the recovery process affects ONLY the application's Primary Production Site – all other public services infrastructure (fire, ambulance, police, etc.) remain intact in the surrounding area. Stated simply, large-scale regional disasters impacting multiple processing facilities are beyond the scope of each application's DR Plan.
- Worst-case scenario is total destruction of the application's Primary Production Site and all application-specific data and hardware housed there. If the actual disaster is not worst-case scenario, procedures may be modified within the appropriate strategies to only cover those critical business processes affected by the disaster-level incident.
- Backup copies of appropriate vital data records have been maintained in a secure off-site storage facility. The off-site storage location is unaffected by the disaster since distance and accessibility were considered in site selection.
- The application and business owners understand the RTO and RPO for their application(s) including the potential data loss due to the RPO. Their application(s) can handle potential data loss, or they have methods to manually recreate the data in the impacted application following recovery.
- Operating efficiency may be reduced during the recovery and stabilization periods. Processing may take longer, communications may be lost or misdirected, and/or there may be greater instances of human error during survival-mode operation.
- All existing physical and data security measures will be implemented into the plan for recovery. No existing security measure will be excluded for emergency processing purposes without prior approval from the UHG IT Information Risk Management Director.

Annual Plan Update Process

DR Plans are reviewed and updated at a minimum, on an annual or biennial basis.

The Application DR Coordinators, in conjunction with their Disaster Recovery Lead and Enterprise DR Coordinator review, update and approve their plans. Once the plans have been approved, the Enterprise DRC posts the plans on an internal (secured) replicated shared storage space.

Individual DR Plans are not provided to outside parties for security reasons. For a contractual or regulatory requirement, these are handled on a per request basis where other options are provided.

DR Plan Approval Process

Every critical application throughout the UnitedHealth Group enterprise requires annual or biennial approval by Application leadership. Generally, the person approving the plan is the owner of the application within the IT organization. EDR manages the process for leadership review the DR Plans and obtain their signoff on the plans for certification purposes. Approval is completed and track using an internal system.

DR Plan Exercise

The Enterprise DR team facilitates the methodology to plan, conduct, evaluate, and manage disaster recovery exercises for Optum Technology. The objectives of DR exercises are to enhance and maintain:

- Stakeholder and regulatory confidence
- Compliance with multiple regulatory requirements (HIPAA, SOX, SAS 70, etc.).
- Contractual commitments made to our customers, vendors, partners, etc.
- Continuous improvement of the exercise methodology, procedures, and deliverables.
- Ability to support business continuation in the event of a disaster.

DR Plans for identified critical business applications and infrastructure are exercised annually. DR exercise results are documented and classified as Confidential. Exercise results are retained according to UnitedHealth Group Records Retention Policy, reported to senior UnitedHealth Group leadership and Business Owners of the affected Corporate and Business Segments, and include remediation plans to address identified gaps.

The following options are available to address the different DR capabilities and regulatory guidelines as appropriate. Depending on multiple factors, any solution below can be applied to meet annual exercise requirements.

- Integrated Functional - Restore multiple applications, allowing end-to-end processes to be executed between applications, individually or as a whole.
- Functional - Restore a single application allowing applicable processes (usually transactions) to be executed within that single system.
- Infrastructure – Restore application systems or infrastructure at recovery location with limited validation of the system state but without application validation.
- Tabletop - Using existing application DR Plans only, simulate a disaster scenario and discuss participant responses.

Communication during a Crisis

Once a disaster has been declared and plans have been activated, there are several groups and individuals who need to be notified a disaster situation has occurred, as well as those who need to be notified the application is unavailable and given a timeframe of when it will be available for use. Notification may include internal staff, external vendors or suppliers and customers and clients.

Definition of a Disaster

A disaster is an event of such magnitude that it threatens the ability of UnitedHealth Group to provide critical business functions and/or services for an extended period of time, including the possibility of causing unacceptable interruption in the Segment/Site’s essential business processes. A disaster may create serious impact to human life/safety issues, security, and/or business viability.

Examples of a disaster include: a full outage of a primary production data center, where the hardware and/or infrastructure is unusable, and recovery is not immediate; or a partial outage of a primary production data center that impacts critical primary IT infrastructure for an extended period of time. An incident is an event which may be, or may lead to, a disaster. However, an incident is never “upgraded” to a disaster without a disaster declaration.

Disaster Declaration

For an event to be declared a disaster, a disaster declaration must be made by an Optum Technology Executive Leader through the Technology Event Management (TEM) process. TEM is managed within Optum Technology’s Technology Command Center which is staffed 24x7x365. When a disaster is declared, the DR Plans will be activated.

A disaster declaration is the formal identification of an event of such severity as to warrant the implementation of business continuity and DR Plans. A disaster declaration provides authorization to execute third party contingency contracts where applicable.

If a disaster has not been declared, the recovery from a systems disruption would be handled as an incident – and the Technology Command Center (TCC) standard processes would be followed.

Priority of Recovery

Once a disaster has been declared, the technical resources will immediately begin the restoration of infrastructure and identified business critical applications for all the different DR capabilities. When a resource is constrained, the prioritization of the resources is based on the recovery time objective documented with the DR plans. Actual recovery priorities may be altered based on additional information available at time of recovery.

Notification with External Customers

No information is to be communicated without prior approval from the Global Crisis Management Team.
No external communication is to be issued without approval from the Global Crisis Management Team.
All media requests must be immediately directed to UnitedHealth Group Corporate Communications.